第一章

非线性周期序列

§1 引　言

本章所讨论的非线性周期序列是指非线性反馈移位寄存器序列与周期随机序列及其样本值，重点是移位寄存器序列。

关于移位寄存器序列（线性或非线性的）已有许多专著及论文进行过讨论，在本章中我们将概述其中的一些结果，对若干与本书特别有关的问题，如 M-序列的构造与计数问题等，将给以完整的叙述与详细的论证；对有些常见的结论，则给以简单的描述。

1.1 关于移位寄存器序列的记号与意义

设 F_q 为一个 q 值的有限域，记

$$\tilde{a}=(a_0, a_1, a_2, \cdots), a_i \in F_q \tag{1-1-1}$$

为 F_q 上的无穷序列，若存在正整数 p，使

$$a_i = a_{i+p}, \quad i=0, 1, 2. \cdots. \tag{1-1-2}$$

成立，则称 $\tilde{a}$ 为周期序列，使(1-1-2) 成立的最小正整数 p 为 $\tilde{a}$ 的周期。若 p 为 $\tilde{a}$ 的周期，则称

$$a^{(p)}=(a_0, a_1, \cdots, a_{p-1}) \tag{1-1-3}$$

为 $\tilde{a}$ 的一个周期，这时由 $a^{(p)}$ 确定全部 $\tilde{a}$。

记 $x^{(n)}=(x_1, x_2, \cdots, x_n)$ 为一个 n 维变元向量，每个 x_i 为在 F_q 上取值的变元，因此 $x^{(n)}$ 为一个在 $F_q^{(n)}$ 上取值的变元，其中

$$F_q^{(n)}=\prod_{i=1}^{n} F_{qi},\quad F_{qi}=F_q \tag{1-1-4}$$

是 F_q 上的 n 维向量空间。如

$$b_{i_1\cdots i_n}\in F_q,\quad i_j\in F_q,\ j=1, \cdots, n$$

为一组在 F_q 中取值的系数，则称

$$\begin{aligned} f(x^{(n)})&=f(x_1, x_2, \cdots, x_n)\\ &=\sum_{j=1}^{n}\sum_{i_j\in F_q} b_{i_1\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \end{aligned} \tag{1-1-5}$$

为 F_q 上的 n 元非线性组合函数，或为 q 值 n 元的布尔函数，其中 x^i 为 x 的 i 次幂（F_q 域中），称

$$b_{i_1\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$$

为 $f(x^{(n)})$ 的 $(i_1, \cdots, i_n)$ 项，而

$$O(i_1, \cdots i_n)=i_1\oplus i_2\oplus\cdots\oplus i_n \tag{1-1-6}$$

为 $(i_1, \cdots, i_n)$ 项的阶，其中“$\oplus$”为实数加法运算。

$$\begin{aligned} \partial^0 f(x^{(n)})\overset{*}{=}&\mathrm{Max}\{O(i_1, \cdots, i_n): i_j\in F_q, j=1, \cdots, n;\\ &b_{i_1\cdots i_n}\neq 0\} \end{aligned} \tag{1-1-7}$$

为 $f(x^{(n)})$ 的阶，其中“$\overset{*}{=}$”表示等式右边的运算在实数域中进行。若 $\partial^0 f(x^{(n)})=1$，则称 $f(x^{(n)})$ 为线性函数，这时 $f(x^{(n)})$ 变为

$$f(x^{(n)})=b_0+b_1x_1+\cdots+b_nx_n。 \tag{1-1-8}$$

在线性移位寄存器理论中，线性运算函数可用多项式

$$f(x)=b_nx+b_{n-1}x^2+\cdots+b_1x^n \tag{1-1-9}$$

表示。

如 $q=2$，则 $i_j=0$ 或 1，因此(1-1-5)的 $f(x^{(n)})$ 变为

$$\begin{aligned} f(x^{(n)})=&b_0+\sum_{i=1}^{n}b_ix_i+\sum_{1\le i<j\le n}b_{ij}x_ix_j\\ &+\cdots+b_{1\cdots n}x_1\cdots x_n \end{aligned} \tag{1-1-10}$$

的形式。它的线性表达式仍为 (1-1-8) 的形式，而 (1-1-10) 的"∑"为按项的阶数组合求和。

我们将 (1-1-5) 的 $f(x^{(n)})$ 对某个变量，如对 x_n 进行幂级数展开，这时 $f(x^{(n)})$ 关于 x_n 的幂级数展开式为

$$f(x^{(n)}) = f_0(x^{(n-1)}) + x_n f_1(x^{(n-1)}) + \cdots + x_n^{q-1} f_{q-1}(x^{(n-1)}), \quad (1\text{-}1\text{-}11)$$

其中

$$f_j(x^{(n-1)}) = f_j(x_1, \cdots, x_{n-1}), \ j = 0, 1, \cdots, q-1$$

为 $n-1$元布尔函数，这时称$(f_0, \cdots, f_{q-1})$为 $f(x^{(n)})$关于 x_n 的幂级数展开系数。

定义 1 (i) 在展开式(1-1-11)中，如果

$$(f_1(x^{(n-1)}), \cdots, f_{q-1}(x^{(n-1)})) \neq (\overbrace{0, \cdots, 0}^{q-1}),$$

则称 $f(x^{(n)})$关于 x_n 变元是非退化的，否则是退化的。

(ii) 称 $f(x^{(n)})$ 为周期序列 $\tilde{a}$ 的 n 级移位寄存器的生成函数(简称生成函数)，如果对任何 $t = 0, 1, 2, \cdots$，

$$a_t = f(a_{t-n}, a_{t-n+1}, \cdots, a_{t-1}) \quad (1\text{-}1\text{-}12)$$

成立，若 $t-j<0$，则取

$$a_{t-n} = a_{t-n+tp}, \ ip \geqslant n-t,$$

其中 p 为 $\tilde{a}$ 的周期。

(iii) 称 $\tilde{a}$ 为一个 q 值 n 级非线性移位寄存器序列，若存在一个关于 x_1 非退化的 $f(x^{(n)})$，使 $f(x^{(n)})$ 为 $\tilde{a}$ 的生成函数。

关于定义 1，在移位寄存器理论中常用的术语与性质说明有：

(1) 若 $f(x^{(n)})$ 为 $\tilde{a}$ 的生成函数，则有时就称 $f(x^{(n)})$ 生成 $\tilde{a}$，或 $\tilde{a}$ 由 $f(x^{(n)})$生成；若 $f(x^{(n)})$ 为线性函数，则 (1-1-12) 就变为

$$a_t = b_0 + b_1 a_{t-n} + \cdots + b_n a_{t-1}, \quad (1\text{-}1\text{-}13)$$

这时 $f(x^{(n)})$关于 x_1 非退化的充要条件为 $b_1 \neq 0$。在线性移位寄

存器理论中常取 $b_0=0$，这时(1-1-13)就变为

$$a_t-(b_1a_{t-n}+\cdots+b_na_{t-1})=0, \qquad (1\text{-}1\text{-}13\alpha)$$

这时记

$$g(x)=1-f(x)=1-b_nx-\cdots-b_1x^n, \qquad (1\text{-}1\text{-}14)$$

为线性移位寄存器的联系多项式。由此可知，联系多项式与生成函数在定义上略有不同。

(2) 在定义 1(i)中，$f(x^{(n)})$关于 x_n 非退化的定义可推广到任何变元 x_i 的情形，对此不作详细描述了。若 $f(x^{(n)})$关于 x_i 退化，则 $f(x^{(n)})$ 变为 $f(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n)$，这是一个与 x_i 无关的函数。

若 $f(x^{(n)})$关于 x_1 退化，则相应的移位寄存器退化为 $n-1$ 级。这个结论对其他的变元 x_i 不成立。例如

$$f(x^{(n)})=x_1,$$

这时相应的移位寄存器仍为 n 级的。

由 $f(x^{(n)})$确定的 n 级非线性反馈移位寄存器如图 1-1 所示。

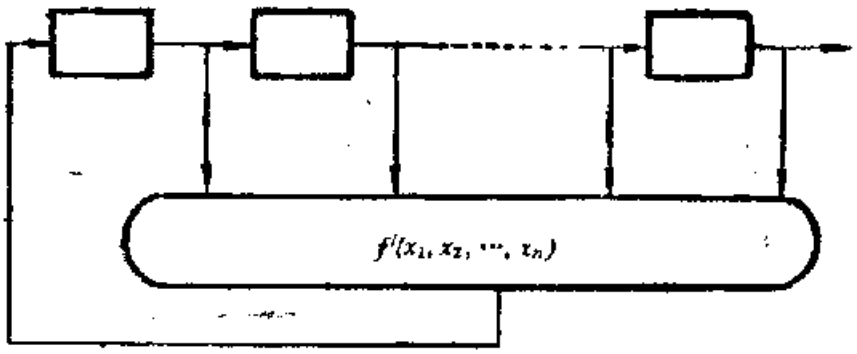


图 1-1 由 $f(x^{(n)})$ 确定的 n 级非线性反馈移位寄存器

因为 $f(x^{(n)})$ 与非线性反馈移位寄存器相互唯一确定，因此我们有时直接称 $f(x^{(n)})$ 为非线性反馈移位寄存器，或该寄存器的运算子。构成 $f(x^{(n)})$ 运算的基本运算与逻辑元件有：和，数乘，变元积$(x_1\cdot x_2)$，幂等。在 $q=2$ 的情形，有“非”运算 $(\bar{x}=1+x)$及“与”、“或”、“非”运算等，它们分别表示为

$$x\wedge y=\begin{cases}0, x=y=0,\\ 1, \text{否则},\end{cases}\qquad x\vee y=\begin{cases}1, x=y=1,\\ 0, \text{否则}.\end{cases}$$

对这些运算在移位寄存器理论中已有详述。如 $f(x^{(n)})$ 是线性的，那么运算由线性元件：和与数乘构成，因此线性移位寄存器由图 1-2 与 1-3 构成，其中图 1-3 为 $q=2$ 的情形。

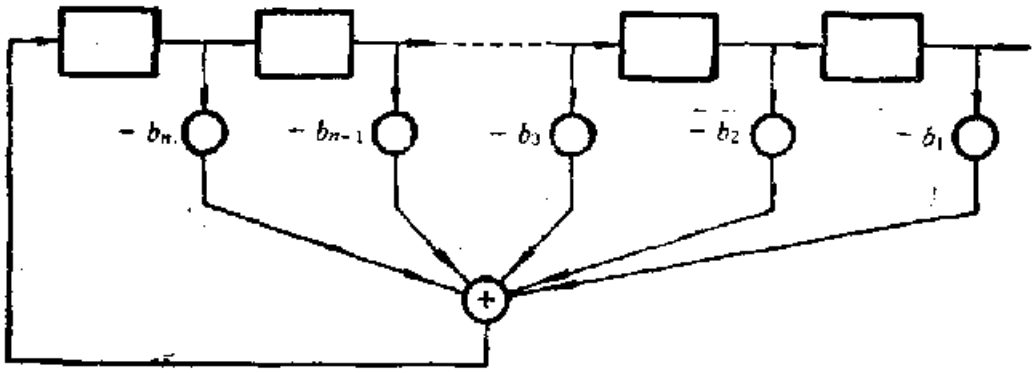


图 1-2　n 级线性反馈移位寄存器

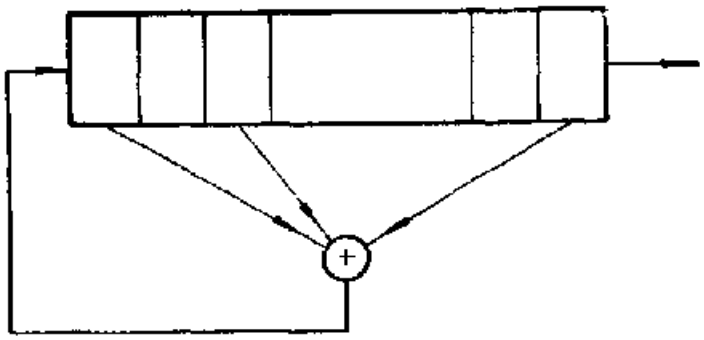


图 1-3　n 级二值线性反馈移位寄存器

1.2　周期随机序列的描述

如果一个序列的分量在 F_q 上取值是随机的，它们具有一定概率分布，这时我们称该序列为随机序列，並记为

$$\tilde{X}=(X_0, X_1, X_2, \cdots),\qquad (1\text{-}1\text{-}15)$$

这时对任何一组下标不同的 $(X_{i_1}, \cdots, X_{i_k})$ 为一个随机向量。它们取 $(a_{i_1}, \cdots, a_{i_k})\in F_q^{(k)}$ 的概率为

$$P_r\{X_{i_1}, \cdots, X_{i_k})=(a_{i_1}, \cdots, a_{i_k})\}.\qquad (1\text{-}1\text{-}16)$$

以下我们称 $\tilde{X}$ 为完全随机的。

(1) $X_0, X_1, X_2, \cdots$ 是一组独立的随机变量。这时(1-1-16)的概率分布为乘积分布

$$\prod_{j=1}^{k} P_r\{X_{i_j}=a_{i_j}\}。 \tag{1-1-17}$$

(2) 每个 X_i 在 F_q 上取均匀分布，这时

$$P_r\{X_i=a_i\}\overset{*}{=}\frac{1}{q} \tag{1-1-18}$$

对任何 $i=0, 1, 2, \cdots$ 成立。

因为在本书中我们讨论的随机序列均是完全的，因此在以下所称的随机序列均为完全随机序列。

定义 2 称 $\widetilde{X}$ 为一周期随机序列，若存在一个正整数 p，使

(i) $X_0, X_1, \cdots, X_{p-1}$ 为一组独立分布且每个 X_i 在 E_q 上取均匀分布的随机变量。

(ii) 对任何 $i=0, 1, 2, \cdots$，总有一个正数 p 存在，使

$$X_i = X_{i+p}$$

成立。以上等式为两随机变量相等(或几乎处处相等)。

使(ii)成立的最小的 p 为 $\tilde{a}$ 的周期。

周期随机序列 $\widetilde{X}$ 可能取的值为一个 F_q 上的序列 $\tilde{a}$，这时称 $\tilde{a}$ 为 $\widetilde{X}$ 的一个样本值，如 $\widetilde{X}$ 周期为 p，则它的样本值是周期序列，且周期小于等于 p。

由移位寄存器理论知，任何有限级反馈移位寄存器序列必为周期序列。因此无论是移位寄存器序列还是周期随机序列的样本值，它们都是周期序列，我们将对此进行讨论。

1.3 周期序列的复杂度问题

关于周期序列的线性与非线性复杂度在许多文献中均有定义，它们有

定义 3 (i) $\tilde{a}$ 的线性复杂度为

$$C_L(\tilde{a})\triangleq\min\{n: \text{存在(1-1-8)的线性函数 } f(x^{(n)}) \text{ 生成 } \tilde{a}\}, \tag{1-1-19}$$

$f(x^{(n)})$生成 $\tilde{a}$ 的定义为(1-1-12)所给。

(ii) $\tilde{a}$ 的非线性复杂度为

$$C_N(\tilde{a}) \triangleq \min \{n: \text{存在(1-1-5)的非线性组合函数 } f(x^{(n)}) \text{生成 } \tilde{a}\}。 \quad (1-1-20)$$

因为我们讨论的均是周期序列,因此对定义式(1-1-19),(1-1-20)可稍作更改,若记

$$a^{(p)} = (a_0, a_1, \cdots, a_{p-1})$$

为 F_q 上的 p 维向量,则我们有

定义 3' (i) 称 $f(x^{(n)})$为 $a^{(p)}$ 的生成函数,如(1-1-12)式对任何 $n \leqslant t < p$ 成立。

(ii) 向量 $a^{(p)}$的线性复杂度为

$$C_L(a^{(p)}) \triangleq \min \{n: \text{存在(1-1-8)的线性函数 } f(x^{(n)}) \text{生成} a^{(p)}\}。 \quad (1-1-21)$$

(iii) $a^{(p)}$ 的非线性复杂度为

$$C_N(a^{(p)}) \triangleq \min \{n: \text{存在(1-1-5)的非线性函数 } f(x^{(n)}) \text{生成 } a^{(p)}\}。 \quad (1-1-22)$$

在序列密码学中,对线性复杂度 $C_L(a^{(p)})$ 已有许多讨论,它们是序列密码学的重要指标,在本书中我们将进一步讨论非线性复杂度问题。

§2 线性复杂度的若干问题

2.1 概述

在序列密码理论中,线性复杂度是序列密码体制的一个重要指标,无论在密码的设计与分析中,任何一个新体制的出现,首先要指明它的线性复杂度。由此可见线性复杂度的重要意义,分析其原因大体上有以下两个方面。

首先,关于一个序列$\tilde{a}$的线性复杂度与线性移位寄存器的综合

解问题，已为 Berlekamp-Massey 算法解决。该算法(以下简称为 B-M 算法)是一个求任意 q 值向量 $a^{(p)}$ 的线性复杂度与生成多项式的快速递推算法，因此对线性复杂度较低的序列，可很快由 B-M 算法找到它的线性复杂度与 $a^{(p)}$ 的生成线性移位寄存器。

另一方面，由线性移位寄存器的条件可知，一个向量 $a^{(p)}$，如果线性复杂度 $C_L(a^{(p)}) \leqslant \frac{1}{2}p$，那么它的线性移位寄存器解是唯一的，因此当 $p \geqslant 2C_N(a^{(p)})$ 时，由 B-M 算法得到的解是唯一的，这样我们就可以获得 $a^{(p)}$ 的唯一生成函数。

由此可见，线性复杂度的指标给出了一个序列密码体制的否定指标，即线性复杂度低的序列密码体制一定是不可靠的，它很快会被 B-M 算法攻破(即找到该序列的生成线性移位寄存器)，因此是不可使用的。

上述结论的反命题不一定成立，即线性复杂度高的序列加密体制不一定是可靠的，大量非线性模型说明了这个问题，对此我们在非线性复杂度理论中再作进一步分析。情况虽然如此，但线性复杂度理论仍不失为序列密码学中的重要基础。在本节中，我们重点介绍 B-M 算法与线性移位寄存器的剩余度问题，以及随机序列的平均线性复杂度与计数分布问题。

2.2 Berlekamp-Massey 算法

该算法由 Berlekamp-Massey 给出，在许多有关序列密码、移位寄存器理论与代数编码的书中均有详细论述。这里介绍它的主要运算步骤。

定义 对已给向量 $a^{(n)}=(a_0, a_1, \cdots, a_{n-1})$，称 $\langle l_n, f_n(x)\rangle$ 为 $a^{(n)}$ 的线性复杂度的综合解(简称线性综合解)，如果：

(i) $l_n=C_L(a^{(n)})$ 为 $a^{(n)}$ 的线性复杂度；

(ii) $f_n(x)$ 为 $a^{(n)}$ 的联系多项式，$\delta^\circ f(\cdot)\leqslant l_n$。

一般来说，我们称求 $a^{(n)}$ 的线性复杂度是指求 $a^{(n)}$ 的线性综

合解，也就是我们不仅要知道 $a^{(n)}$ 的线性复杂度，还要知道 $a^{(n)}$ 的生成函数。在一般情形下，$a^{(n)}$ 的生成函数是不唯一的，在综合解问题中，我们只要求出其中之一即可。关于求全体生成函数的问题，我们将在以下几节中讨论，这个问题称为移位寄存器的剩余问题。

B-M 算法的基本思想是一个递推运算过程，设

$$a^{(p)}=(a_0, a_1, \cdots, a_{p-1}),\ a_i\in F_q \tag{1-2-1}$$

为一个已知的 q 值向量。若 $n\leqslant p-1$，记

$$a^{(n)}=(a_0, a_1, \cdots, a_{n-1})$$

为 $a^{(p)}$ 的一个部分向量(或为 $a^{(p)}$ 的前段向量)，B-M 算法的递推过程就是由已知的 $a^{(n)}$ 向量的综合解 $\langle l_n, f_n(x)\rangle$，及 $a^{(p)}$ 的数据递推计算 $\langle l_{n+1}, f_{n+1}(x)\rangle$。B-M 算法的运算步骤为：

BM-Ⅰ　取 $n_0\geqslant 1$，使

$$a_0=a_1=\cdots=a_{n_0-1}=0,\ a_{n_0}\neq a_0.$$

这时取

$$d_0=d_1=\cdots=d_{n_0-1}=0,\ d_{n_0}=a_{n_0},$$

且取

$$\begin{cases} f_1(x)=f_2(x)=\cdots=f_{n_0}(x)\equiv 1,\\ l_1=l_2=\cdots=l_{n_0}=0, \end{cases} \tag{1-2-2}$$

$f_{n_0+1}(x)$ 为任一 n_0+1 阶多项式，如

$$\begin{cases} f_{n_0+1}(x)=1-d_{n_0}x^{n_0+1},\\ l_{n_0+1}=n_0+1, \end{cases} \tag{1-2-3}$$

这时 $\langle l_n, f_n(x)\rangle$ 为 $a^{(n)}$ 的线性综合解，其中 $n=1, 2, \cdots, n_0+1$。

BM-Ⅱ　已知 $\langle l_i, f_i(x)\rangle$ 为 $a^{(i)}$ 线性综合解，$i=1, 2, \cdots, n$，且有

$$l_1=l_2=\cdots=l_{n_0}\leqslant l_{n_0+1}\leqslant l_{n_0+2}\leqslant\cdots\leqslant l_n, \tag{1-2-4}$$

这时就可由 $\langle l_i, f_i(x)\rangle$，$i=1, 2, \cdots, n$ 及 $a^{(p)}$ 求 $\langle l_{n+1}, f_{n+1}(x)\rangle$。

若记

$$f_i(x)=1+b_{i1}x+b_{i2}x^2+\cdots+b_{il_i}x^{l_i},\qquad (1\text{-}2\text{-}5)$$

$$i=1,2,\cdots,n,$$

这时可定义

$$d_n=a_n+b_{n1}a_{n-1}+\cdots+b_{nl_n}a_{n-l_n},\qquad (1\text{-}2\text{-}6)$$

且必有以下两种情况之一发生，即

$$d_n=0 \quad 或 \quad d_n\neq 0.$$

对此我们有

(1) 如果 $d_n=0$，这时就取

$$\langle l_{n+1},f_{n+1}(x)\rangle=\langle l_n,f_n(x)\rangle,\qquad (1\text{-}2\text{-}7)$$

(2) 如果 $d_n\neq 0$，这时总有一个 $m<n$，使

$$l_m<l_{m+1}=l_{m+2}=\cdots=l_n\qquad (1\text{-}2\text{-}8)$$

成立，由 $\langle l_i,f_i(x^{(i)})\rangle$ 的条件可知，这样的 m 必存在。因此我们就可作

$$\begin{cases} f_{n+1}(x)=f_n(x)-d_nd_m^{-1}x^{n-m}f_m(x),\\ l_{n+1}=\max\{l_n,n-l_n+1\}. \end{cases}\qquad (1\text{-}2\text{-}9)$$

这时 $\langle l_{n+1},f_{n+1}(x^{(l_{n+1})})\rangle$ 由(1-2-7)与(1-2-9)确定。

BM-Ⅲ 重复 BM-Ⅱ 的步骤，所得$\langle l_i,f_i(x)\rangle$必使(1-2-4)成立，这样对 $n<p$ 的解，总可递推计算得到 $n+1\leqslant p$ 的解，直到 $n=p$ 为止，这时 $\langle l_p,f_p(x)\rangle$ 就为所求。

以上这个运算步骤就是 B-M 算法。

定理 1 对已知的 $a^{(p)}$ 向量，由以上 BM-Ⅰ，Ⅱ，Ⅲ 的步骤求得的 $\langle l_p,f_p(x)\rangle$必为 $a^{(p)}$ 的线性综合解。

该定理的详细证明可见[1]，这里不作详述了。另外，在[1]中还可见到利用 B-M 算法求 $a^{(p)}$ 综合解的例子。例如

$$a^{(11)}=(00100011101)\qquad (1\text{-}2\text{-}10)$$

的线性综合解为

$$l_{11}=6,\ f_{11}(x^{(6)})=1+x^2+x^3+x^4+x^5.$$

若

$$a^{(15)}=(000100110101111), \qquad (1\text{-}2\text{-}11)$$

则相应的线性综合解为

$$\langle l_{15}, f_{15}(x)\rangle=\langle 4, 1+x^3+x^4\rangle.$$

详细计算过程可见[1]文 300 页例 1 与例 2.

2.3　线性移位寄存器的剩余度问题

在 B-M 算法中,我们已给出了由已知向量 $a^{(p)}$ 求综合解 $\langle l_p, f_p(x)\rangle$ 的运算步骤,从这些运算步骤中可知，当 $a^{(p)}$ 给定时,线性复杂度 $l_p=C_N(a^{(p)})$ 是唯一确定的，但线性移位寄存器 $f_p(x)$ 的解可能不唯一，因此线性移位寄存器的剩余度问题就是求已知 $a^{(p)}$ 的全部线性移位寄存器 $f_p(x)$ 的解,对此有

定理 2　如果向量 $a^{(p)}=(a_0, a_1, \cdots, a_{p-1})$ 的线性复杂度 $C_L(a^{(p)})=n\overset{*}{\geqslant}\frac{1}{2}p$, 那么状态向量组

$$s_i=(a_i, a_{i+1}, \cdots, a_{i+n-1}) \quad (i=0, 1, \cdots, p-n) \qquad (1\text{-}2\text{-}12)$$

是线性无关的.

证明　我们用反证法。若(1-2-12)线性相关，这时有一组 $b_1, b_2, \cdots, b_{p-n}\in F_q$, 使

$$s_{p-n}=b_1 s_{p-n-1}+b_2 s_{p-n-2}+\cdots+b_{p-n-1}s_0$$

成立，这时有

$$\begin{cases} a_{p-1}=b_1 a_{p-2}+b_2 a_{p-3}+\cdots+b_{p-n} a_{n-1}, \\ a_{p-2}=b_1 a_{p-3}+b_2 a_{p-4}+\cdots+b_{p-n} a_{n-2}, \\ \cdots\cdots \\ a_{p-n}=b_1 a_{p-n-1}+b_2 a_{p-n-2}+\cdots+b_{p-n}a_0 \end{cases} \qquad (1\text{-}2\text{-}13)$$

成立,这时 $a^{(p)}$ 的线性复杂度为

$$C_L(a^{(p)})\overset{*}{\leqslant}p-n\overset{*}{\leqslant}n-1,$$

这与 $C_L(a^{(p)})=n$ 的假定矛盾. 定理得证.

推论　在定理 2 条件下，若 $p\overset{*}{<}2n$,则生成 $a^{(p)}$ 的线性移位寄存器有 q^{2n-p} 多个.

证明 如果

$$f_p(x)=b_1x+b_2x^2+\cdots+b_nx^n \tag{1-2-14}$$

为 $a^{(p)}$ 的生成多项式，这时关系式

$$\begin{cases} a_n=b_1a_{n-1}+b_2a_{n-2}+\cdots+b_na_0, \\ a_{n+1}=b_1a_n+b_2a_{n-1}+\cdots+b_na_1, \\ \cdots\cdots \\ a_{p-1}=b_1a_{p-2}+b_2a_{p-3}+\cdots+b_na_{p-n-1} \end{cases} \tag{1-2-15}$$

成立，由定理 2 知，(1-2-15)的系数矩阵为

$$\begin{bmatrix} a_{n-1}, a_{n-2}, \cdots, a_0 \\ a_{n-2}, a_{n-1}, \cdots, a_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{p-2}, a_{p-3}, \cdots, a_{p-n-1} \end{bmatrix}$$

的秩为 $p-n$，因此方程(1-2-15)中 b_i ($i=1, 2, \cdots, n$) 的解有 q^{2n-p} 多个。

当 $p\geqslant^{*}2n=^{*}2C_L(a^{(p)})$时，在[1]等文中给出了相应的结论，这时有

定理 3 如果 $p\geqslant^{*}2n=^{*}2C_L(a^{(p)})$，那么 $a^{(p)}$ 的线性移位寄存器综合解 $\langle n, f_p(x)\rangle$ 是唯一的，且它必可由 B-M 算法产生。

该定理在[1]文第三章 §8 的定理 2 与定理 1 中已有详细讨论，对此不再重述。

如记 $N_L(a^{(p)})$ 为 $a^{(p)}$的线性移位寄存器的综合解的个数，则由上面推论与定理 3 可得

$$N_L(a^{(p)})=^{*}\begin{cases} q^{2n-p}, & \text{当 } p\leqslant 2n-1 \text{ 时}, \\ 1, & \text{当 } p>2n-1 \text{ 时}, \end{cases} \tag{1-2-16}$$

其中 $n=C_L(a^{(p)})$。

以上 B-M 算法及定理 1～3 反映了向量 $a^{(p)}$ 的线性移位寄存器综合解的性质。以下我们讨论在 p, n 固定时，使 $C_L(a^{(p)})=n$ 成立的 $a^{(p)}$ 的计数分布与相应的平均特征。

2.4　随机序列的平均线性复杂度与分布计数公式

如果 $X^{(p)}=(X_0, X_1, \cdots, X_{p-1})$为随机向量，$X_i$ 为独立同分布且在 F_q 上取均匀分布，它的样本值为 $a^{(p)}=(a_0, a_1, \cdots, a_{p-1})$。因为对每个 $a^{(p)}$ 有线性复杂度 $C_L(a^{(p)})$，因此 $C_L(X^{(p)})$为一个随机变量。以下我们称

$$p_L(n)\triangleq P_r\{C_L(X^{(p)})=n\} \qquad (n=0, 1, 2, \cdots, p) \quad (1\text{-}2\text{-}17)$$

为 $C_L(X^{(p)})$ 的概率分布，而

$$E\{C_L(X^{(p)})\}\overset{*}{=}\sum_{n=0}^{p} np_L(n)$$

$$\overset{*}{=}\sum_{a^{(p)}\in F_q^{(p)}}\left[\frac{1}{q^p}C_L(a^{(p)})\right] \quad (1\text{-}2\text{-}18)$$

为 $X^{(p)}$ 的平均线性复杂度。同样，我们可以定义 $C_L(X^{(p)})$ 的公差

$$D[C_L(X^{(p)})]\overset{*}{=}\sum_{n=0}^{p}[n-E\{C_L(X^{(p)})\}]^2P_L(n). \quad (1\text{-}2\text{-}19)$$

在[7]、[11]等文中给出了 $p_L(n)$，$E\{C_L(X^{(p)})\}$，$D[C_L(X^{(p)})]$ 的一系列计算。在 $q=2$ 的情形，对其中有关要点概述如下：

(1) 定义

$$\tilde{N}_p(n)\overset{*}{=}\{a^{(p)}\in F^{(p)}, C_L(a^{(p)})\equiv n\},$$

且记 $N_p(n)=\|\tilde{N}_p(n)\|$，则关于 $N_p(n)$ 的递推与计数公式为

$$N_p(n)\overset{*}{=}\begin{cases}2N_{p-1}(n)+N_{p-1}(p-n), & p\geqslant n>\dfrac{p}{2}\text{ 时},\\ 2N_{p-1}(n), & p=2n\text{ 时},\\ N_{p-1}(n), & p>2n>0.\end{cases} \quad (1\text{-}2\text{-}20)$$

由(1-2-20)即可推出 $N_p(n)$ 的计数公式为

$$N_p(n)\overset{*}{=}\begin{cases}\exp_2\{\min(2p-2n, 2n-1)\}, & p\geqslant n>0,\\ 1, & p>n=0,\end{cases} \quad (1\text{-}2\text{-}21)$$

因此

$$p_L(n)\overset{*}{=}\frac{1}{2^p}N_p(n)\overset{*}{=}\begin{cases}\exp_2\{\min(p-2n,\ 2n-p-1)\}, & \text{当 } p\geqslant n>0 \text{ 时}\\ 1, & \text{当 } p>n=0 \text{ 时}.\end{cases}\tag{1-2-22}$$

这就是 $C_L(X^{(p)})$ 的概率分布公式。

(2) 由关系式 (1-2-18)、(1-2-19)、(1-2-22) 即可得到 $C_L(X^{(p)})$ 的均值与方差,它们是

$$E\{C_L(X^{(p)})\}\overset{*}{=}\frac{p}{2}+\frac{4+R_2(p)}{18}+2^{-p}\left(\frac{p}{3}+\frac{2}{9}\right),\tag{1-2-23}$$

其中

$$R_2(p)=\begin{cases}0, & \text{若 } p \text{ 为偶数},\\ 1, & \text{若 } p \text{ 为奇数},\end{cases}$$

而

$$D[C_L(X^{(p)})]\overset{*}{=}\frac{86}{81}-2^{-p}\left[p\frac{14-R_2(p)}{27}+\frac{82-2R_2(p)}{81}\right]-2^{-2p}\left(\frac{1}{9}p^2+\frac{4}{27}p+\frac{4}{81}\right).\tag{1-2-24}$$

由此可知,当 p 较大时,

$$E\{C_L(X^{(p)})\}\cong\frac{p}{2}+\frac{4+R_2(p)}{18},$$

$$D[C_L(X^{(p)})]\cong\frac{86}{81}.$$

这些公式的推导过程可见[11],在此不再详述。

§3 非线性反馈移位寄存器的表示

一个 n 级非线性反馈移位寄存器有以下几种表示方法,即函数表示、列表表示、组合表示与图表示。现在概述有关表示的记号与性质。

3.1 函数表示

用(1-1-5)的非线性组合函数来表示非线性反馈移位寄存器,这时 $f(x^{(n)})$ 是一个

$$F_q^{(n)} \to F_q \qquad (1\text{-}3\text{-}1)$$

的映射. 特殊情形,如 $f(x^{(n)})$ 为线性函数或 $q=2$ 的情形,相应的 $f(x^{(n)})$ 为(1-1-8)与(1-1-10)所示。另一方面,由布尔函数的性质知道,任何(1-3-1)的映射总可表示为(1-1-5)的函数形式,对此我们作以下论述.

(1) 若 $n=1$,这时(1-1-5)的 $f(x^{(n)})$ 变为

$$f(x)=b_0+b_1x+\cdots+b_{q-1}x^{q-1}. \qquad (1\text{-}3\text{-}2)$$

这时有

引理 1 对 F_q 上的 $q-1$ 阶多项式 $f(x)\equiv 0$ 的充要条件为

$$b_0=b_1=\cdots=b_{q-1}=0.$$

证明 充分性是显然的,证必要性即可。如果 $f(x)\equiv 0$,则当 $x=0$ 时,必有

$$f(x)=b_0=0,$$

因此

$$f(x)=x(b_1+b_2x+\cdots+b_{q-1}x^{q-2})\equiv 0$$

成立。这时对任何非零的 x 有

$$b_1+b_2x+\cdots+b_{q-1}x^{q-2}=0 \qquad (1\text{-}3\text{-}3)$$

成立。记 α 为 F_q 的一个本原元,这时 F_q 的全体非零元为

$$\alpha,\ \alpha^2,\ \cdots,\ \alpha^{q-2},\ \alpha^{q-1}=e,$$

其中 e 为 F_q 的幺元。这时方程(1-3-3)变为方程组

$$b_1+b_2\alpha^i+\cdots+b_{q-1}\alpha^{i(q-2)}=0,$$

$$i=1,\ 2,\ \cdots,\ q-1. \qquad (1\text{-}3\text{-}4)$$

如把 b_i 看作未知数,这时方程组(1-3-4)的系数矩阵行列式为

$$\begin{vmatrix} 1, \alpha, & \alpha^2, & \cdots, \alpha^{q-2} \\ 1, \alpha^2, & \alpha^4, & \cdots, \alpha^{2(q-2)} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 1, \alpha^{q-1}, & \alpha^{2(q-1)}, & \cdots, \alpha^{(q-1)(q-2)} \end{vmatrix}$$

$$= \prod_{1 \le i < j \le n} (\alpha^i - \alpha^j) \neq 0, \qquad (1\text{-}3\text{-}5)$$

因此方程组(1-3-4)有唯一解，即必有 $b_1 = b_2 = \cdots = b_{q-1} = 0$。在(1-3-5)中的行列式为 $q-1$ 阶 Vandermonde(范德蒙德)行列式，它的值为(1-3-5)右边的形式(详细证明见[1]中定理6)。引理得证。

引理 2 任何一个 $F_q \to F_q$ 的映射均可表示为(1-3-2)的多项式，而且在 $\partial^\circ f(x) \leqslant q-1$ 条件下表示式是唯一的。

证明 我们记全体(1-3-2)的多项式集合为 $\mathscr{F}_q$，这时

$$\mathscr{F}_q = \{f(x) = b_0 + b_1 x + \cdots + b_{q-1}x^{q-1}: \\ b_i \in F_q, i = 1, 2, \cdots, q-1\}。 \qquad (1\text{-}3\text{-}6)$$

由引理1知，对任何 $f_1(x) \neq f_2(x) \in \mathscr{F}_q$，为 $F_q \to F_q$ 的两个不同映射，因此 $\mathscr{F}_q$ 的元与全体 $F_q \to F_q$ 的映射是1-1对应的。这时 $\|\mathscr{F}_q\|$($\mathscr{F}_q$ 的元素个数)与全体 $F_q \to F_q$ 的映射个数均为 q^q 个。因此每一个 $F_q \to F_q$ 的映射均可表示为 $\mathscr{F}_q$ 的一个元，而且表示式是唯一的，引理得证。

以下我们称

$$\chi_a(x) = \begin{cases} 1, & \text{若 } x = a, \\ 0, & \text{否则} \end{cases} \qquad (1\text{-}3\text{-}7)$$

为 a 上的特征函数。这时 $\chi_a(x)$ 必可表示为

$$\chi_a(x) = \prod_{a' \neq a} \frac{(a' - x)}{(a' - a)}, \qquad (1\text{-}3\text{-}8)$$

这时我们只要将 $x = a$，$x \neq a$ 分别代入(1-3-8)就可得到(1-3-7)成立。(1-3-8)为特征函数的一般表示式。对于 $q = 2$ 的情形，

(1-3-8)变为

$$\chi_a(x)=x+a+1。\qquad(1-3-9)$$

(2) 为讨论一般 $f(x^{(n)})$情形,同样可定义

$$\mathscr{F}_q^{(n)}=\{\text{全体(1-1-5)的非线性组合函数 } f(x^{(n)})\},$$

$$\mathscr{T}_q^{(n)}=\{\text{全体 } F_q^{(n)}\to F_q \text{ 的映射}\}。\qquad(1-3-10)$$

定理 1　$\mathscr{F}_q^{(n)}$与$\mathscr{T}_q^{(n)}$是两个1-1对应的集合,即对于任何$\mathscr{T}_q^{(n)}$中的元 $T^{(n)}$, 必有一个 $f(x^{(n)})\in\mathscr{F}_q^{(n)}$,使 $T^{(n)}(x^{(n)})=f(x^{(n)})$,且是唯一的。反之, 任何 $f(x^{(n)})\in\mathscr{F}_q^{(n)}$ 为 $\mathscr{T}_q^{(n)}$ 的元且 1-1 对应。

证明　因为 $\mathscr{F}_q^{(n)}$ 与 $\mathscr{T}_q^{(n)}$ 的元素个数相同, 为

$$\|\mathscr{F}_q^{(n)}\|=\|\mathscr{T}_q^{(n)}\|=q^{q^n},\qquad(1-3-11)$$

因此只要证明 $\mathscr{F}_q^{(n)}$ 与 $\mathscr{T}_q^{(n)}$ 是 1-1 对应的即可。为此, 只要证 $f(x^{(n)})\equiv 0$ 的充要条件为

$$b_{i_1\cdots i_n}=0,\ \text{对任何 } i_j\in F_q,\ j=1,\cdots,n。$$

我们用归纳法证明这个结论。

首先对 $n=1$ 时,上述充要条件为引理 1, 因此当 $n=1$ 时命题成立。

若 $n-1$ 时命题成立,证明在 n 时命题成立。同样充分性是显然的, 只要证必要性即可。由关系式(1-1-11)可知, $f(x^{(n)})$ 可按 x_n 的幂展开,这时

$$f_j(x^{(n-1)})=\sum_{r=1}^{n-1}\sum_{i_r\in F_q} b_{i_1\cdots i_n j}x_1^{i_1}\cdots x_{n-1}^{i_{n-1}},$$

$$j=0,1,\cdots,q-1。\qquad(1-3-12)$$

如 $f(x^{(n)})\equiv 0$, 则就 x_n 而言,由引理 1 知,对任何 x_1, $\cdots$, x_{n-1}, 必有

$$f_0(x^{(n-1)})\equiv f_1(x^{(n-1)})\equiv\cdots\equiv f_{q-1}(x^{(n-1)})\equiv 0。$$

又由归纳法假定及(1-3-12)知, 这时必有

$$b_{i_1,\cdots i_{n-1},j}=0,\ \text{对任何 } i_r\in F_q,\ r=1,\cdots,n-1,$$

$$j=0,1,\cdots,q-1,\qquad(1-3-13)$$

必要性得证，定理成立。

同样，我们可以引进 $a^{(n)}$ 上的特征函数

$$\chi_{a^{(n)}}(x^{(n)})=\begin{cases}1, & \text{若 } x^{(n)}=a^{(n)},\\ 0, & \text{否则。}\end{cases}$$

这时 $\chi_{a}{}^{(n)}(x^{(n)})$ 的表示式为

$$\chi_{a^{(n)}}(x^{(n)})=\prod_{i=1}^{n}\chi_{a_i}(x_i), \tag{1-3-14}$$

其中 $\chi_a(x)$ 为 (1-3-7) 定义的特征函数，而

$$a^{(n)}=(a_1,\cdots,a_n),\ x^{(n)}=(x_1,\cdots,x_n)。$$

以下我们把 $\mathscr{F}_q^{(n)}$ 与 $\mathscr{T}_q^{(n)}$ 看作同一集合，$f(x^{(n)})$ 与 $T^{(n)}$ 看作同一元素。

3.2 列表表示与组合表示

如果直接将映射

$$f(x^{(n)}):F_q^{(n)}\to F_q \tag{1-3-15}$$

列成函数表，则称之为列表表示。如 $q=2$ 时，函数

$$f(x^{(3)})=1+x_1+x_2+x_1x_2x_3$$

可由表 1 表示。

表 1 $1+x_1+x_2+x_1x_2x_3$ 的列表表示

$x^{(3)}$	$f(x^{(3)})$
0 0 0	1
0 0 1	1
0 1 0	0
1 0 0	0
0 1 1	0
1 0 1	0
1 1 0	1
1 1 1	0

在(1-3-15)映射中,我们定义

$$A_a[f(x^{(n)})]=\{x^{(n)}: f(x^{(n)})=a\}, \tag{1-3-16}$$

这时

$$A_F[f(x^{(n)})]=\{A_a[f(x^{(n)})], a\in F_q\} \tag{1-3-17}$$

为 $F_q^{(n)}$ 的一组分割,即

$$A_a[f(x^{(n)})]\bigcap A_{a'}[f(x^{(n)})]=\varnothing(\text{空集}),$$

对任何 $a\neq a'\in F_q$ 成立,且

$$\bigcup_{a\in Fq} A_a[f(x^{(n)})]=F_q^{(n)}.$$

以下我们记

$$A[f(x^{(n)})]=\bigcup_{a\neq 0} A_a[f(x^{(n)})]. \tag{1-3-18}$$

因此当 $q=2$ 时,

$$A_1[f(x^{(n)})]=A[f(x^{(n)})], A_0[f(x^{(n)})]=A[f(x^{(n)})]^c. \tag{1-3-19}$$

在本书中,我们称 $A_F[f(x^{(n)})]$ 为 $f(x^{(n)})$ 的组合表示。在 $q=2$ 时,称 $A_0[f(x^{(n)})]$(或 $A_1[f(x^{(n)})]$)为 $f(x^{(n)})$的组合表示。

定理 2 $A_F=\{A_a, a\in F_q\}$ 为 $F_q^{(n)}$ 的一组分割,则必存在一个(1-1-5)的 $f(x^{(n)})$,使

$$A_F[f(x^{(n)})]=A_F \tag{1-3-20}$$

成立,且 $f(x^{(n)})$具有唯一的表达式

$$f(x^{(n)})=\sum_{\substack{a\in Fq\\ a\neq 0}}\left\{a\sum_{a^{(n)}\in A_a}\left[\prod_{i=1}^{n}\prod_{a'\neq a_i}\frac{(a'-x_i)}{(a'-a_i)}\right]\right\}. \tag{1-3-21}$$

证明 A_F 为 $F_q^{(n)}$ 的一组分割,则必存在且唯一的一个 $F_q^{(n)}\to F_q$ 的映射 $f(x^{(n)})$,使(1-3-20)成立。另一方面,又由特征函数的定义可知,使(1-3-20)成立的 $f(x^{(n)})$必为

$$f(x^{(n)})=\sum_{\substack{a\in Fq\\ a\neq 0}}\{a\sum_{a^{(n)}\in A_a}\chi_{a^{(n)}}(x^{(n)})\}, \tag{1-3-22}$$

将(1-3-14),(1-3-8)代入(1-3-22),即得(1-3-21)成立,定理得证。

3.3 图表示

非线性反馈移位寄存器的图表示理论在许多文献中均有论述，在本书中也有较多的讨论，对此先介绍有关的术语、记号与性质。

(1) 关于图的一般定义：

称 $G=\{A, L\}$为一个有限图，若A 为某个有限集合，它的元称为图的顶点或点，L 为 A 的部分点偶的集合，它的元为弧。以下记

A 的元为 s, t, u, v 等；

L 的元为 $(s, t), (u, v)$等。

在 L 中，若 (s, t) 与 (t, s) 看作同一弧，则 G 为无向图，否则为有向图。有时我们又记 L 的弧为 S, V 等。

在有向图中，如 $S=(s, t)$ 为弧，这时称：S 为 s 的出弧，t 的入弧；s 为 t 的先导，t 为 s 的后继；s 为 S 的前端，t 为 S 弧的末端。

若 $S=(s, t)$, $S'=(t, u)$，则称 S, S' 为相连的弧，t 为连结点。若干相连的弧为路。G 的路记为

$$W=\{S_1, S_2, \cdots, S_k\}=\{s_0, s_1, \cdots, s_k\}, \qquad (1\text{-}3\text{-}22)$$

其中

$$S_i=(s_{i-1}, s_i), i=1, 2, \cdots, k.$$

对(1-3-22)的路，我们称 s_0 为起点，s_k 为终点；S_1 为起弧，S_k 为末弧。$S_1, \cdots, S_k$ 为 W 依次经过的弧，$s_0, s_1, \cdots, s_k$ 为 W 依次经过(或到达)的点。如 $s_k=s_0$，则称 W 为一回路。如

$$S=(s, s)\in L,$$

则称 S 为一环。对任何 $s, t\in A$，若有一条路将 s, t 相连，则称从 s 可到达 t。

在回路 W 中，若它经过的弧 $S_1, \cdots, S_k$ 互不相同，则称 W 为单回路；若它经过的顶点 $s_0, s_1, \cdots, s_{k-1}$ 互不相同，则称 W 为初等回路或圈。经过 G 的所有弧的回路为完备回路，又称为 Euler 回路。经过 G 的所有顶点的圈为极大圈，又称为 Hamiltom 回路。

路(或圈)中弧的个数称为路(圈)长。

以下记 $d^+(s)$为 G 图中在 s 点的入弧数，$d^-(s)$为 s 点的出弧数。若对任何顶点 $s\in A$，总有

$$d^+(s)=d^-(s)=q,$$

则称 G 为一个 q- 图。

如果 $G=\{A, L\}$，$G'=\{A', L'\}$ 为两个图，且 $A'\subset A$，$L'\subset L$，这时称 G' 为 G 的子图或部分图。

(2) de Bruijn-Good 有向图：

在图 $G=\{A, L\}$的定义中，如

$$A=F_q^{(n)},\quad L=F_q^{(n+1)}, \tag{1-2-23}$$

这时称 G 为 de Bruijn-Good 有向图，并记为 $G_n(q)=\{A_n(q), L_n(q)\}$，有时简记为 $G_n=\{A_n, L_n\}$。

显然 G_n 是一个 q- 图，它的每个顶点为

$$s=a^{(n)}=(a_0, a_1, \cdots, a_{n-1}),\quad a_i\in F_q,$$

有时我们称之为状态。G_n 的弧为

$$\begin{aligned}S=a^{(n+1)}&=(a_0, a_1, \cdots, a_{n-1}, a_n)\\&=((a_0, a_1, \cdots, a_{n-1}), (a_1, a_2, \cdots, a_n)),\end{aligned} \tag{1-3-24}$$

因此 G_n 的弧为状态在移位寄存器中可能转移的向量。

一个非线性反馈移位寄存器 $f(x^{(n)})$ 可看作一个部分 de Bruijn-Good 有向图，这时 $A=F_q^{(n)}$，而

$$L=\{S=(a^{(n)}, f(a^{(n)})): a^{(n)}\in F_q^{(n)}\}. \tag{1-3-25}$$

为了与 G_n 的记号表示区别，我们记(1-3-25)的 L 为 $L[f(x^{(n)})]$，相应的非线性反馈移位寄存器图记为

$$G[f(x^{(n)})]=\{A_n, L[f(x^{(n)})]\}. \tag{1-3-26}$$

显然，$G[f(x^{(n)})]$ 为 G_n 的一个子图，每个顶点 $a^{(n)}$ 有且只有一条出弧。

定理 3 若 $G=\{A, L\}$为 G_n 的一个子图，$A=F_q^{(n)}$，且每个顶点在 G 中有且只有一条出弧，这时必有一个 n 元非线性组合函

数 $f(x^{(n)})$，使

$$G[f(x^{(n)})]=G.$$

证明 若 G 为 G_n 的子图，且 G 的每个顶点有且只有一条出弧，如记 $a^{(n)}=(a_0,\cdots,a_{n-1})$ 为 G 的一个顶点，则它的出弧为

$$(a_0,a_1,\cdots,a_{n-1},a_n(a_0,\cdots,a_{n-1}))\in L,$$

其中 $a_n(a_0,\cdots,a_{n-1})\in F_q$，这时

$$f(x_1,\cdots,x_n)=a_n(x_1,\cdots,x_n)$$

就是 $F_q^{(n)}\to F_q$ 的一个映射，有

$$L[f(x^{(n)})]=L,\ G[f(x^{(n)})]=G.$$

定理得证。

(3) 关于 $G[f(x^{(n)})]$ 图的若干性质。

定理 3 已经给出了 $G[f(x^{(n)})]$ 图的基本构造性质，由此可以得到 $G[f(x^{(n)})]$ 图的若干描述性质。

定理 4 (i) $G[f(x^{(n)})]$ 图至少存在一个圈(或环)。

(ii) $G[f(x^{(n)})]$ 图中每个顶点必达到该图中的某个圈(或环)。

(iii) $G[f(x^{(n)})]$图中不同的圈无公共点，且每个顶点只能达到一个圈中的点。

(iv) 若记 $W_i,i=1,\cdots,r$，为 $G[f(x^{(n)})]$图中所有的圈，又记

$$\widetilde{W}_i=\{G[f(x^{(n)})]\text{ 中可达到 }W_i\text{ 的全体顶点}\},$$

则 $\widetilde{W}_1,\cdots,\widetilde{W}_r$ 为 $F_q^{(n)}$ 的一个分割。

证明 该定理性质(iv)由(iii)即可推出，因此我们只要证(i)—(iii)即可。

关于性质(i)，(ii)，由 $G[f(x^{(n)})]$ 的全体顶点的有限性及每个顶点总有一条出弧，可知性质(i)，(ii)必须成立，否则会出现无限多个顶点，与 $G[f(x^{(n)})]$ 图的定义矛盾。

对性质(iii)可用反证法证。若

$$W_1=\{s_0,s_1,\cdots,s_{k+1}\},\ W_2=\{t_0,t_1,\cdots,t_{k'+1}\}$$

为两个不同的圈，$s_0=s_{k+1}$，$t_0=t_{k'+1}$。如它们有一个公共点，即$s_0=t_0$，它们的后继 s_1，t_1 也必相同，因为在 $G[f(x^{(n)})]$ 图中，$s_0=t_0$ 点只有一条出弧，这时 $s_1=t_1$。同理可得

$$s_2=t_2,\ s_3=t_3,\ \cdots,$$

最后必有 $k'=k$，且 $W_1=W_2$，与假设矛盾。

同样可得，任何 s 点只可能到达一个圈中的点。若 s 可达到不同圈 W_1，W_2 中的两个点 s_0，t_0，这时 W_1，W_2 必有公共点，与 $G[f(x^{(n)})]$ 图中不同圈无公共点的性质矛盾。定理得证。

定理 4 对 $G[f(x^{(n)})]$ 图中顶点的运动情形进行分类，以下称

$$\mathfrak{W}_1,\ \mathfrak{W}_2,\ \cdots,\ \mathfrak{W}_r \qquad (1\text{-}3\text{-}27)$$

为 $G[f(x^{(n)})]$ 图运动状态分割类，这时每个 $\mathfrak{W}_i$ 的点经过若干次状态转移，结果必到达 $\mathfrak{W}_i$ 中的圈 W_i，而每个 $G[f(x^{(n)})]$ 的点转移结果必到达某个圈 W_i。

引理 3　若 $\mathfrak{W}_i\neq W_i$，则 $\mathfrak{W}_i$ 中必有若干个顶点只有出弧没有入弧。

该引理的证明由 $\mathfrak{W}_i$ 顶点的有限性及它只含一个圈的定义即得。对此不再详述。

定义　在 $G[f(x^{(n)})]$ 图中，只有出弧没有入弧的点称为梢点。

没有梢点的 $G[f(x^{(n)})]$ 为非奇异的非线性移位寄存器，相应的 $f(x^{(n)})$ 称为非奇异函数。

如果 $G[f(x^{(n)})]$ 只有一个极大圈构成，这时称 $G[f(x^{(n)})]$ 为 M-序列图，或称 $f(x^{(n)})$ 为 M-序列生成函数。

一个 n 级非线性移位寄存器序列，若周期为 q^n，则这个序列为 M-序列。

如果 $f(x^{(n)})$ 为 M-序列的生成函数，则对任何初始状态 $(a_0, a_1, \cdots, a_{n-1})$，由 $f(x^{(n)})$ 产生的移位寄存器序列 $(a_0, a_1, a_2, \cdots)$ 总是 M-序列，这时 a_i 满足关系式(1-1-12)。

关于非奇异移位寄存器与 M-序列生成函数的一系列性质，在后文中还有详细论述。

(4) 关于 G_n 图中状态的几种运算。若 $s=(a_0, a_1, \cdots, a_{n-1}) \in F_q^{(n)}$，这时定义 s 上的几种运算为

(i) 共轭运算。如果 τ 为 $F_q \to F_q$ 的映射，则称

$$s_\tau^* = (\tau(a_0), a_1, \cdots, a_{n-1})$$

为 s 的共轭运算，相应的 s_τ^* 为 s 的共轭元，而

$$\tilde{s}^* = \{(a_0', a_1, \cdots, a_{n-1}) : a_0' \in F_q\} \qquad (1\text{-}3\text{-}28)$$

为 s 的共轭元组，共轭元组 $\tilde{s}^*$ 中每个与 s 不同的元为 s 的共轭元。

当 $q=2$ 时，s 的共轭元为

$$s^* = (a_0+1, a_1, a_2, \cdots, a_{n-1}). \qquad (1\text{-}3\text{-}29)$$

(ii) 相伴运算。对上述 s 与 τ，同样定义

$$s_\tau' = (a_0, \cdots, a_{n-2}, \tau(a_{n-1}))$$

为 s 的相伴运算，称

$$\tilde{s}' = \{(a_0, \cdots, a_{n-2}, a_{n-1}') : a_{n-1}' \in F_q\} \qquad (1\text{-}3\text{-}30)$$

为 s 的相伴元组，$\tilde{s}'$ 中每个与 s 不同的元为 s 的相伴元。

当 $q=$ 时，s 的相伴元为

$$s' = (a_0, a_1, \cdots, a_{n-2}, a_{n-1}+1). \qquad (1\text{-}3\text{-}31)$$

(iii) 反运算。对 $s=(a_0, a_1, \cdots, a_{n-1})$ 定义它的反运算为

$$D(s) = (a_{n-1}, a_{n-2}, \cdots, a_0). \qquad (1\text{-}3\text{-}32)$$

(iv) 补运算。对 $q=2$ 的 s 定义它的补运算为

$$\bar{s} = (\bar{a}_0, \bar{a}_1, \cdots, \bar{a}_{n-1}),$$

其中 $\bar{a}_i = a_i + 1$。同样对于 F_2 中的 n 维变元 $x^{(n)} = (x_1, \cdots, x_n)$ 可定义它的补元为

$$\bar{x}^{(n)} = (\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n).$$

还可以定义 $x^{(n)}$ 中部分分量的补元，如 $x^{(n)}$ 关于 x_1, x_2 的补元为

$$(\bar{x}_1, \bar{x}_2, x_3, x_4, \cdots, x_n).$$

这时，这些变元的运算也可由补元代替，如

$$\bar{x}_1\bar{x}_2x_3x_4\bar{x}_5=(1+x_1)(1+x_2)x_3x_4(1+x_5),\quad (1\text{-}3\text{-}33)$$

这时关于 $a^{(n)}$ 的特征函数就可直接由(1-3-33)的函数来写出，如

$$a^{(5)}=(01001),$$

则

$$\chi_{a^{(5)}}(x^{(5)})=\bar{x}_1x_2\bar{x}_3\bar{x}_4x_5.$$

§4 非线性反馈移位寄存器的若干基本性质

4.1 非奇异移位寄存器的性质

一个非线性移位寄存器的 de Bruijn-Good 图 $G[f(x^{(n)})]$ 的非奇异性已在本章§3中定义，现在介绍它们的性质。

定理1 在 $q=2$ 时，以下条件相互等价：

(i) $f(x^{(n)})$ 是非奇异的。

(ii) $G[f(x^{(n)})]$ 由若干个圈构成。

(iii) $G[f(x^{(n)})]$ 的每个点有且只有一条入弧。

(iv) $f(x^{(n)})=x_1+f_0(x_2,x_3,\cdots,x_n)$。

(v) $A[f(x^{(n)})]^*=A[f(x^{(n)})]^c$，其中

$$A[f(x^{(n)})]=\{x^{(n)}:f(x^{(n)})=1\},$$

$$A^c=F_2^{(n)}-A,\ A^*=\{s^*:s\in A\}.$$

也就是 $A[f(x^{(n)})]$ 等于它余集的共轭。我们称这个性质为 $A[f(x^{(n)})]$ 的厄米性。

证明 (i)～(iv)的等价性在[2]中已有详细证明，以下证(iv)或(v)的等价性。

关于(iv)，(v)的等价性是易证的。因为若(iv)成立，则对于任何 $x^{(n)}\in A_1[f(x^{(n)})]$ 总有

$$f(x^{(n)*})=\bar{x}_1+f_0(x_2,\cdots,x_n)=1+1=0,$$

此即

$$x^{(n)*}\in A_0[f(x^{(n)})]=A_1[f(x^{(n)})]^c,$$

则性质(v)成立。反之,如(v)成立,这时作

$$f_0(x_2, \cdots, x_n) = f(0, x_2, \cdots, x_n),$$

$$f_1(x_1, \cdots, x_n) = x_1 + f_0(x_2, \cdots, x_n),$$

只要证明 $f_1(x^{(n)}) \equiv f(x^{(n)})$ 即可。这时

$$A_1[f_1(x^{(n)})] = A_1[f_1(x^{(n)})]_{x_1=0} \bigsqcup A_1[f_1(x^{(n)})]_{x_1=1},$$

其中

$$A_{x_1=a} = (x_1 = a) \otimes A[x_1 = a],$$

而

$$A[x_1 = a] = \{(x_2, \cdots, x_n) : (a, x_2, \cdots, x_n) \in A\}$$

为 A 在 $x_1 = a$ 上的切口。另外,如 $A \in F_2^{(m)}$, $B \in F_2^{(n)}$,则

$$A \otimes B = \{(x^{(m)}, y^{(n)}) : x^{(m)} \in A, y^{(n)} \in B\}.$$

由 $f_1(x^{(n)})$ 的定义知

$$A_1[f_1(x^{(n)})]_{x_1=0} = (x_1 = 0) \otimes A_1[f_0(x_2, \cdots, x_n)]$$

$$= A_1[f(x^{(n)})]_{x_1=0},$$

又由性质(v)知

$$A_1[f_1(x^{(n)})]_{x_1=1} = (x_1 = 1) \otimes A_0[f_0(x_2, \cdots, x_n)]$$

$$= \{A_0[f(x^{(n)})]_{x_1=0}\}^* = A_1[f(x^{(n)})]_{x_1=1},$$

因此

$$A_1[f_1(x^{(n)})] = A_1[f(x^{(n)})]_{x_1=0} \bigsqcup A_1[f(x^{(n)})]_{x_1=1}$$

$$= A_1[f(x^{(n)})].$$

成立,此即

$$f(x^{(n)}) = f_1(x^{(n)}) = x_1 + f_0(x_2, \cdots, x_n)$$

成立,(iv)式得证。

定理 1 的等价条件可推广到一般 q 值的情形,这时我们更改定理 1 中的 (iv), (v)条件为:

(iv′) 函数 $f(x_1, x_2, \cdots, x_n)$ 为 x_1 的 1-1 对应函数,这时对任何 $x_2, \cdots, x_n$, 如 $x_1 \neq x_1'$ 时,

$$f(x_1, x_2, \cdots, x_n) \neq f(x_1', x_2, \cdots, x_n).$$

(v′)　$A_F[f(x^{(n)})]$ 为 $F_q^{(n)}$ 的一个共轭元组。

如 $A_F=\{A_a, a\in F_q\}$ 为 $F_q^{(n)}$ 的一个分割，且对任何 $(a_2, \cdots, a_n)\in F_q^{(n-1)}$，

$$(a_1, a_2, \cdots, a_n),\ a_1\in F_q$$

分别属于 A_a, $a\in F_q$ 的一个集合。

定理 2　对一般 q 值的非线性移位寄存器条件(i)、(ii)、(iii)、(iv′) 与 (v′) 必相互等价，其中条件 (i), (ii), (iii)为定理 1 所定义。

该定理的证明与定理 1 相似，对此不再详述。

推论 1　q 值 n 元的非奇异函数有

$$N_s(n, q)\triangleq(q!)^{q^{n-1}} \tag{1-4-1}$$

多个。

证明　由定理 2 知，$f(x^{(n)})$为非奇异的充要条件是对任何$(x_2, \cdots, x_n)\in F_q^{(n-1)}$，$f(x_1, x_2, \cdots, x_n)$是 x_1 的 1-1 对应函数，因此$f(x^{(n)})$的取法有$(q!)^{q^{n-1}}$ 多种。它们是全部 q 值 n 元的非奇异函数。

定理 2 给出了一个构造全部 q 值 n 元非奇异函数的方法。它的构造过程如下：

记 SYM(q) 为 $F_q\to F_q$ 的全体置换群，相应的置换函数为 $\sigma(a)$, $a\in F_q$。这时 $\sigma(a)$ 的多项式表示为

$$g_\sigma(x)=\sum_{a\in F_q}\sigma(a)\chi_a(x),$$

其中 $\chi_a(x)$ 为 a 上的特征函数，由(1-3-8)确定。记

$$Q_q=\{g_\sigma(x):\sigma(\cdot)\in\mathrm{SYM}(q)\},$$

定义

$B_q=\{(b_0, b_1, \cdots, b_{q-1})$，如

$$g(x)=b_0+b_1x+\cdots+b_{q-1}x^{q-1}\in Q_q\}. \tag{1-4-2}$$

推论 2　记

$$f(x^{(n)})=f_0(x_2, \cdots, x_n)+x_1f_1(x_2, \cdots, x_n)$$

$$+\cdots+x_1^{q-1}f_{q-1}(x_2,\cdots,x_n),\qquad(1\text{-}4\text{-}3)$$

则 $f(x^{(n)})$ 为非奇异的充要条件是对任何 $(x_2,\cdots,x_n)\in F_q^{(n-1)}$,

$$(f_0(x_2,\cdots,x_n),\cdots,f_{q-1}(x_2,\cdots,x_n))\in B_q.\qquad(1\text{-}4\text{-}4)$$

这个结论由本节定理 2 直接可得。因此为构造非奇异的 $f(x^{(n)})$，我们只要构造 B_q 即可。

定理 3 对 $q>2$ 的情形，如 $(b_0,b_1,\cdots,b_{q-1})\in B_q$，则必有 $b_{q-1}=0$，因此 $f(x^{(n)})$ 为非奇异的一个必要条件为

$$f_{q-1}(x_2,x_3,\cdots,x_n)\equiv 0.\qquad(1\text{-}4\text{-}5)$$

证明 记 $d=\prod_{\substack{a\in F_q\\ a\neq 0}}a$,则有

$$\chi_a(x)=\frac{1}{d}\prod_{a'\neq a}(a'-x)=\frac{1}{d}[(-1)^{q-1}x^{q-1}+h_a(x)],$$

其中 $h_a(x)$为阶数小于等于 $q-2$ 的多项式.如$\sigma(\cdot)\in\mathrm{SYM}(q)$,则

$$q_\sigma(x)=\frac{1}{d}[(-1)^{q-1}x^{q-1}\sum_{a\in F_q}\sigma(a)+\sum_{a\in F_q}\sigma(a)h_a(x)],$$

这时必有

$$\sum_{a\in F_q}\sigma(a)=\sum_{a\in F_q}a=0,$$

$$\partial^0[\sum_{a\in F_q}\sigma(a)h_a(x)]\leqslant q-2,\qquad(1\text{-}4\text{-}6)$$

因此 $q_\sigma(x)$的 $q-1$ 次项系数 $b_{q-1}=0$。此即 (1-4-5) 成立，定理 3 得证。

注意，定理 3 的结果在 [4] 中已经获得。因为这个性质与非奇异函数有关,在此给出叙述与证明。

例 1 对 $q=3$ 情形给出全体非奇异函数。

解 这时 $F_q=\{0,1,2\}$，相应的全体特征函数为

$$\chi_0(x)=2x^2+1,$$

$$\chi_1(x)=2x^2+2x,$$

$$\chi_2(x)=2x^2+x,$$

$\sigma(a)$ 为 $\{0,1,2\}$ 上的置换，有 6 个分别是

$$(0,1,2),\ (0,2,1),\ (1,0,2),$$
$$(1,2,0),\ (2,0,1),\ (2,1,0)。$$

分别记之为 $\sigma_i(\cdot)$，相应的

$$q_i(x)=\sigma_i(0)\chi_0(x)+\sigma_i(1)\chi_1(x)+\sigma_i(2)\chi_2(x),$$

这时全体 $\sigma_i(\cdot)$，$q_i(x)$，(b_{i0},b_{i1}) 可列表如下：

表 2　$q=3$ 时的 σ_i，$q(x)$，$b_1^{(2)}$ 表

i	1	2	3	4	5	6
σ_i	(0,1,2)	(0,2,1)	(1,0,2)	(1,2,0)	(2,0,1)	(2,1,0)
q_i	x	$2x$	$2x+1$	$x+1$	$x+2$	$2x+2$
(b_{i0},b_{i1})	(0,1)	(0,2)	(1,2)	(1,1)	(2,1)	(2,2)

这时

$$B_3=\{(0,1),(0,2),(1,2),(1,1),(2,1),(2,2)\}。$$

因此在 $q=3$ 时，$f(x^{(n)})$ 为非奇异的充要条件为

$$f_2(x_2,\cdots,x_n)\equiv 0,\ f_1(x_2,\cdots,x_n)\not\equiv 0。\qquad (1\text{-}4\text{-}7)$$

例 2　对 $q=4$ 的情形，这时记

$$F_4=\{0,1,\omega,\omega+1\},\ 这里\ \omega^2=\omega+1。$$

求全体非奇异的 $f(x^{(n)})$。

解　相应的特征函数为

$$\chi_0(x)=x^3-1,\ \chi_1(x)=x^3-x^2+x,$$
$$\chi_\omega(x)=x^3-\omega x^1+(\omega+1)x,$$
$$\chi_{\omega+1}(x)=x^3-(\omega+1)x^2+\omega x,$$

记

$$\sigma_i=(\sigma_i(0),\sigma_1(1),\sigma_i(\omega),\sigma_i(\omega+1))$$
$$q_i(x)=\sum_{a\in F_4}\sigma_i(a)\chi_a(x),$$

则全体 σ_i，$q_i(x)$，(b_{i0},b_{i1},b_{i2}) 可列表表示如下：

表 3　$q=4$ 时 σ_i, $q_i(x)$, $b_i^{(s)}$ 表

i	$\sigma_i(a)$	$q_i(x)$	$(b_{i_0}, b_{i_1}, b_{i_2})$
1	0　1　ω　$\omega+1$	x	(0, 1, 0)
2	0　1　$\omega+1$　ω	x^2	(0, 0, 1)
3	0　ω　1　$\omega+1$	ωx^2	(0, 0, ω)
4	0　ω　$\omega+1$　1	ωx	(0, ω, 0)
5	0　$\omega+1$　1　ω	$x^2+(\omega+1)x$	(0, $\omega+1$, ω)
6	0　$\omega+1$　ω　1	$(\omega+1)x$	(0, $\omega+1$, 0)
7	1　0　ω　$\omega+1$	x^2+1	(1, 0, 1)
8	1　0　$\omega+1$　ω	$x+1$	(1, 1, 0)
9	1　ω　0　$\omega+1$	$(\omega+1)x+1$	(1, $\omega+1$, 0)
10	1　ω　$\omega+1$　0	$x^2+(\omega+1)x+1$	(1, $\omega+1$, 1)
11	1　$\omega+1$　0　ω	ωx^2+1	(1, 0, ω)
12	1　$\omega+1$　ω　0	$\omega x+1$	(1, ω, 0)

续表

i	$\sigma_i(a)$	$q_i(x)$	$(b_{i_0}, b_{i_1}, b_{i_2})$
13	ω 0 1 $\omega+1$	$\omega x+\omega$	$(\omega, \omega, 0)$
14	ω 0 $\omega+1$ 1	$\omega x^2 \quad +\omega$	$(\omega, 0, \omega)$
15	ω 1 0 $\omega+1$	$x^2+(\omega+1)x+\omega$	$(\omega, \omega+1, 1)$
16	ω 1 $\omega+1$ 0	$(\omega+1)x+\omega$	$(\omega, \omega+1, 0)$
17	ω $\omega+1$ 0 1	$x+\omega$	$(\omega, 1, 0)$
18	ω $\omega+1$ 1 0	$x^2 \quad +\omega$	$(\omega, 0, 1)$
19	$\omega+1$ 0 1 ω	$x^2+(\omega+1)x+\omega+1$	$(\omega+1, \omega+1, 1)$
20	$\omega+1$ 0 ω 1	$(\omega+1)x+\omega+1$	$(\omega+1, \omega+1, 0)$
21	$\omega+1$ 0 ω 1	$\omega x+\omega+1$	$(\omega+1, \omega, 0)$
22	$\omega+1$ 1 ω 0	$\omega x^2 \quad +\omega+1$	$(\omega+1, 0, \omega)$
23	$\omega+1$ ω 0 1	$x^2 \quad +\omega+1$	$(\omega+1, 0, 1)$
24	$\omega+1$ ω 1 0	$x+\omega+1$	$(\omega+1, 1, 0)$

这时相应的

$$B_4=\{(b_0,1,0),(b_0,0,1),(b_0,0,\omega),(b_0,\omega,0),$$
$$(b_0,\omega+1,1),(b_0,\omega+1,0),\ b_0\in F_4\},$$

因此 $f(x^{(n)})$ 为非奇异的充要条件为在分解式 (1-4-3) 中满足条件：

(i) $f_3(x_2,x_3,\cdots,x_n)\equiv 0$；

(ii) $(f_1(x_2,\cdots,x_n),f_2(x_2,\cdots,x_n))\in\{(1,0),$
$(0,1),(0,\omega),(\omega,0),(\omega+1,1),(\omega+1,0)\}$。

其中条件(ii)可简化为(ii')：

$$f_2(x_2,\cdots,x_n)\equiv 0 \text{ 且 } f_1(x_2,\cdots,x_n)\neq 0,$$

或

$$(f_1(x_2,\cdots,x_n),f_2(x_1,\cdots,x_n))\in\{(0,1),(0,\omega),(\omega+1,1)\}。$$

4.2 移位寄存器的剪接问题

移位奇存器的剪接问题是指在移位寄存器的 de Bruijn-Good 图中改变某些点的出弧，使两个(或多个)不同的圈合并为同一个圈或将同一个圈分解成两个(或多个)不同的圈。

设 $G[f(x^{(n)})]$为一个移位寄存器的 de Bruijn-Good图，如

$$s=(a_0,a_1,\cdots,a_{n-1}),\ s^*=(a_0^*,a_1,\cdots,a_{n-1})$$

为两个 $F_q^{(n)}$ 中的共轭元，$a_0\neq a_0^*\in F_q$，它们在 $G[f(x^{(n)})]$中的后继点为

$$t=(a_1,\cdots,a_{n-1},a_n),\ t'=(a_1,\cdots,a_{n-1},a_n'),$$

若 $f(x^{(n)})$ 是非奇异的，则必有 $a_n\neq a_n'\in F_q$，或 t，t' 为 $F_q^{(n)}$ 中的两个相伴元。我们改变移位寄存器 $f(x^{(n)})$，使 (s,t)，(s^*,t') 弧变为弧 (s,t')，(s^*,t)，而其余的弧保持不变，这时就称之为移位寄存器的剪接运算，并记为

$$J\{s,t;s^*,t'\}$$
$$=J\{(s,t)\to(s,t');(s^*,t')\to(s^*,t)\}。\qquad (1\text{-}4\text{-}8)$$

关于剪接运算有有以下性质。

定理 4 对移位寄存器 $f(x^{(n)})$ 进行剪接运算 $J\{s, t; s^*, t'\}$，这时有

(i) 若 $f(x^{(n)})$ 是非奇异的，则剪接后的图仍为非线性移位寄存器的 de Bruijn-Good 图，且仍为非奇异的。

(ii) 若记 $f_1(x^{(n)})$ 为 $f(x^{(n)})$ 经 $J\{s, t; s^*, t'\}$ 剪接后的移位寄存器，则

$$f_1(x^{(n)}) = f(x^{(n)}) + \chi_{(a_0,a_0^*)}(x_1)[f(s^*) - f(s)] \cdot [\prod_{i=1}^{n-1} \chi_{a_i}(x_{i+1})], \tag{1-4-9}$$

其中

$$f(s) = f(a_0, a_1, \cdots, a_{n-1}),$$

$$\chi_{(a,a^*)}(x) = \begin{cases} 1, & \text{如 } x = a, \\ -1, & \text{如 } x = a^*, \\ 0, & \text{如 } x \neq a, a^*. \end{cases} \tag{1-4-10}$$

证明 我们记 $G[f(x^{(n)})]$ 经过剪接后的图为 G_J，这时显然有：

(i) G_J 为移位寄存器的 de Brujin-Good 图。因为在 G_J 中每一个顶点仍有且只有一条出弧，记相应的运算函数为 $f_1(x^{(n)})$。

(ii) 若 $f(x^{(n)})$ 为奇异的，则 $G[f(x^{(n)})]$ 的每个点有且只有一条入弧，这时 G_J 的每个点有且只有一条入弧，因此 $f_1(x^{(n)})$ 也是奇异的。

(iii) 由 $f_1(x^{(n)})$ 定义即得

$$f_1(x^{(n)}) = \begin{cases} f(x^{(n)}), & \text{若 } x^{(n)} \neq s, s^*, \\ f(s^*), & \text{若 } x^{(n)} = s, \\ f(s), & \text{若 } x^{(n)} = s^*, \end{cases} \tag{1-4-11}$$

记(1-4-9)右边第二项为 $J(s, s^*; x^{(n)})$，则有

$$J(s,s^*;x^{(n)})=\begin{cases}0, & \text{若 } x^{(n)}\neq s,\ s^*,\\ f(s^*)-f(s), & \text{若 } x^{(n)}=s,\\ f(s)-f(s^*), & \text{若 } x^{(n)}=s^*,\end{cases}$$

因此 (1-4-9) 成立，这时 $f_1(x^{(n)})$为 G_f 图的运算函数。定理得证。

以下定理给出剪接运算的图形性质。

定理 5 在定理 4 的条件与记号下，如果弧 (s, t),(s^*,t') 分别在两个不同圈中，则 $G[f_1(x^{(n)})]$图将这两个圈并成一个圈。反之，若 (s, t), (s^*, t') 弧在同一个圈中，则 $G[f_1(x^{(n)})]$将这个圈分成两个不同的圈。

证明 我们记 $G[f(x^{(n)})]$ 的两个圈为

$$(s_0=s, s_1=t, s_2, \cdots, s_{l_1}),$$
$$(t_0=s^*, t_1=t', t_2, \cdots, t_{l_2}), \qquad (1\text{-}4\text{-}12)$$

这时它们在 $G[f_1(x_i^{(n)})]$ 图中，s 的后继为 $t_1=t'$, t_2, $\cdots$, t_{l_2}, 而 t_{l_2}的后继为 $t_0=s^*$, s^* 的后继为 $s_1=t$, s_2, $\cdots$, s_{l_1}, $t_0=s$。因此 (1-4-12)的两个圈并成一个圈。

反之，若弧 (s, t), (s^*, t') 在一个圈中，我们记之为

$$(s_0=s, s_1=t, s_2, \cdots, s_{l_1-1}, s_{l_1}=s^*, s_{l_1+1}=t',$$
$$s_{l_1+2}, \cdots, s_{l_1+2}, \cdots, s_{l_1+l_2-1}), \qquad (1\text{-}4\text{-}13)$$

这时在 $G[f_1(x^{(n)})]$ 图中，$s_0=s$ 的后继为：

$$s_0=s\to s_{l_1+1}=t'\to s_{l_1+2}\to\cdots\to s_{l_1+l_2-1}\to s_0,$$

这时$(s_0, s_{l_1+1}, \cdots, s_{l_1+l_2-1}, s_0)$成一个圈，而 $s_{l_1}=s^*$ 的后继分别为

$$s_{l_1}=s^*\to s_1=t\to s_2\to\cdots\to s_{l_1-1}\to s_{l_1}=s^*,$$

这时$(s_{l_1}, s_1, s_2, \cdots, s_{l_1-1}, s_{l_1})$成一个圈，因此(1-4-13)的圈分解成两个圈，定理得证。

在许多文献中，利用上述剪接法来构造 M-序列，如 s 与 s^* 不在同一个圈中，则由剪接运算 $J\{s, t; s^*, t'\}$可将这两个圈合

并，经过若干次剪接运算必可将一个非奇异的移位寄成器变为 M-序列生成器。

以下称 (1-4-9) 的 $f_1(x^{(n)})$ 为 $f(x^{(n)})$ 关于 s, s^* 的置换运算，因为这时有(1-4-11)式成立。同时，在组合表示

$$A_F[f(x^{(n)})] \text{ 与 } A_F[f_1(x^{(n)})]$$

中，s 与 s^* 的位置互换。

以下我们把改变出弧的运算均作为剪接运算，如 $J\{(s, t)\to(s, t')\}$ 就是将(s, t)弧改变为(s, t')弧的运算。因此，一般的剪接运算就可表示为

$$J\{(s_i, t_i)\to(s_i, t_i'), i=1, 2, \cdots, r\}, \quad (1\text{-}4\text{-}14)$$

这就是把弧(s_i, t_i) 变为(s_i, t_i')，$i=1, 2, \cdots, r$，其中 t_i' 为 t_i 的相伴元。

4.3　n 级轮换移位寄存器

记 n 级移位寄存器的非线性函数为

$$f(x_1, x_2, \cdots, x_n)=x_1, \quad (1\text{-}4\text{-}15)$$

这时相应的 n 级反馈移位寄器为图 1-4 所示，它被称为 n 级轮换移位寄存器，并记为 $PCR_n(q)$。

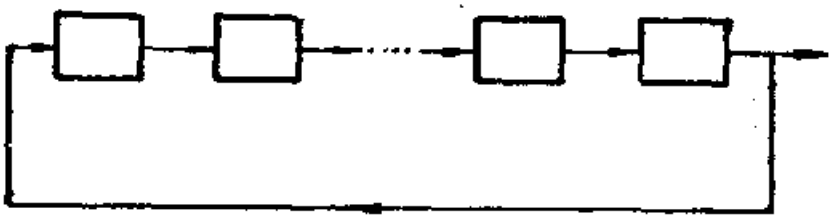


图 1-4　n 级轮换移位寄存器

定理 6　在 $PCR_n(2)$的状态图中，圈的周期(长度)一定是 n 的正因数，如 d 为 n的一个正因数，那么 $PCR_n(2)$图中，周期为 d 的圈的个数为

$$N_n(d)\triangleq\frac{1}{d}\left[\sum_{d':d'\mid d}\mu(d')2^{\frac{d}{d'}}\right], \quad (1\text{-}4\text{-}16)$$

其中从 $\mu(d)$为 Möbius 函数,而状态图的总圈数为

$$z(n)\overset{*}{=}\frac{1}{n}\sum_{d:d|n}\phi(d)2^{\frac{n}{d}}, \qquad (1\text{-}4\text{-}17)$$

$\phi(d)$ 为 Euler 函数,$d'|d$ 为 d' 整除 d,且在(1-4-16)、(1-4-17)中的加、乘、除、幂等运算均在实数中进行(相应的等式用"$\overset{*}{=}$"表示)。

定理 6 的证明及 Möbius 函数、Euler函数的定义与性质均可在[2],[10]等文中找到。

§5 反树图的构造与计数问题

关于 M-序列的构造与计算问题是经典的移位寄存器问题,在许多文献中进行过讨论,为了适应序列密钥的要求,我们进一步讨论这一问题,目的是把 M-序列的构造进一步规范化,使全体 n 级 M-序列以一定密钥空间相对应,且由该密钥空间的参数直接构造或计算相应的 M-序列,这个计算过程应是较容易的。

为了上述目的,我们先介绍关于 M-序列的已有构造方法,即反树图构造方法。为了使本书的讨论能直接进入核心问题,我们在此直接介绍 q 值的 de Bruijn-Good 图与反树图的构造理论。本书中的有关结果可在[5]文中找到。

5.1 反树图的定义与性质

在 §3 中我们已介绍了图的一般定义与它的一系列记号和术语,这些术语在本节完全适用。现在重点讨论一种特殊的图,即反树图。

定义 1 称图 $T=\{A, L\}$为一个反树图(或简称反树),若存在一个顶点 $s_0\in A$,使

(i) 每个非 s_0 的顶点 $s\in A$ 总有且只有一条出弧。

(ii) 顶点 s_0 没有出弧。

(iii) 每个顶点 $s\in A$ 总有一条路，使 s 到达 s_0(若 $s=s_0$，s 自然到达 s_0)。

这时称 s_0 为反树 T 的根。

引理 1 关于反树图有以下性质：

(i) 任何非 s_0 的顶点 $s\in A$，必有且只有一条路到达 s_0。

(ii) 任何反树 T 中必不含圈。

证明 (i) 由反树图定义知，任何非 s_0 的顶点 s 总有一条路可达到 s_0。另一方面，任何 $s\neq s_0$ 的顶点在 T 中只有一条出弧，因此也只有一个后继。这样从 s 出发的路只有一条，且到达终点的路也只有一条，性质(i)得证。

(ii) 若反树图 $T=\{A, L\}$ 中含有一个圈 W，$s_0\in W$，则

$$W=\{s_0, s_1, \cdots, s_k, s_{k+1}=s_0\},$$

这时 $S_i=(s_{i-1}, s_i)$，$i=1, 2, \cdots, k+1$ 为 L 中的弧，s_0 就有一出弧，与 s_0 为根的定义矛盾。

若 $s_0\notin W$，这时在 W 中总有一个点 s_i，使 s_i 点有一出弧 $(s_i, t)\in L$，且 $t\notin W$ (否则，W 中的点都不能到达 s_0)。这时 s_i 就有二条出弧 (s_i, s_{i+1})，$(s_i, t)\in L$，这里 $s_{i+1}\neq t$，与 T 的定义矛盾，因此反树图 T 中必不含圈，引理得证。

引理 1 中(ii)的逆题命也成立。这时有

引理 2 如果 $T=\{A, L\}$ 图具有本节定义 1 的条件 (i)，(ii) 及(iii')，图 T 中不含圈，则 T 为反树图。

证明 该引理证明与引理 1 中 (i) 相似，对于任何一个顶点 $s\neq s_0$，必有一条路，使 s 到达 s_0，否则，由 s 可引出一条无限长的路，这与 A 的有限性矛盾。引理得证。

由引理 1 与引理 2 知，关于反树图的定义条件(i)，(ii)，(iii) 与(i)，(ii)，(iii') 相互等价。我们还可得

推论 在反树图 T 中，至少有一个顶点没有入弧。

证明 若 T 中每个顶点都有入弧，这时可构造一系列

$$s_0, s_1, s_2, \cdots, \tag{1-5-1}$$

其中 s_0 为任取一点，s_1 为 s_0 的先导，s_2 为 s_1 的先导。如此继续，对任何 s_i 总有先导 s_{i+1} 存在，因为 T 中全体顶点有限，因此在(1-5-1)的 s_i 中总有一对(i, j)，使 $s_i = s_j$，$i < j$。这时$(s_i, s_{i+1}, \cdots, s_j)$为 T 中的一个圈，与本节引理 1 中(ii)矛盾。因此 T 中至少有一个顶点没有入弧。推论得证。

在反树图 T 中，没有入弧的顶点为稍点。

定义 2 若 $T = \{A', L'\}$ 为图 $G = \{A, L\}$ 子反树图，则称 T 为 G 的部分反树；若 T 为 G 的部分反树，且 $A' = A$，则称 T 为 G 的极大部分反树图。

下文中所述名词与定义常用到，即：从 s 到根 s_0 的路长为 s 在反树中的层次，因此 s_0 为 T 中零层的顶点。

有两条以上入弧的顶点为反树 T 的一个分权点。没有分权点的反树称为反干树。以下记 $T_s = \{A_S, L_S\}$ 为 T 的一个子图，其中 A_S 为全体 T 中可到达 s 的顶点(包括 s)，L_S 为 A 中除 s 之外全体顶点在 T 中的出弧，称 T_s 为 T 在 s 上的一个分枝。

如 S 为 T 的弧，以下记 $T_S = \{A_S, L_S\}$，其中 $A_S = A_t \cup \{s\}$，$S = (t, s)$，$L_S = L_t \cup \{S\}$。这时称 T_S 为 T 在 S 上的分枝。如 T 在 s 点没有分权，$S = (t, s) \in L$，这时 $T_S = T_s$，否则 T_S 为 T_s 的一个子图。

引理 3 以下条件相互等价：

(i) T_0 为一反干树。

(ii) 反树 T_0 中任何一个顶点最多只有一条入弧。

(iii) 反树 T_0 只有一个稍点。

证明 该引理的证明是明显的，因为由反干树定义知 (i)⇒(ii) 必成立。又由反树定义 1(iii)知，(ii)⇒(iii) 必成立，因为若反树 T_0 有两个稍点 s，t，则这两个点都可到达 s_0，它们之间必不

可达。因此从 s，t 到 s_0 的两条路必在某点汇合，这与本引理条件(ii)矛盾，又由本节推论知，这时 T_0 有且只有一个悬点，故(iii)成立。

若反树 T_0 只有一个悬点，则 T_0 不可能有分权点。如我们记 $\|A\|=k$ 为 T_0 的顶点个数，且 T_0 在 s 处有分权点，因为 T_0 只有一个点没有入弧，所以 $\|L\|\geqslant k$，这与反树定义 $\|L\|=k-1$ 矛盾。因此(iii)⇒(i)成立，引理得证。

5.2　有向图的联系矩阵

对有向图 $G=\{A, L\}$，如记

$$A=\{s_1, s_2, \cdots, s_n\}, \tag{1-5-2}$$

且定义

$$d_{ij}=\begin{cases}1, & \text{若 } (s_j, s_i)\in L,\\ 0, & \text{否则,}\end{cases} \tag{1-5-3}$$

这时我们称矩阵

$$B(G)=[d_{ij}]_{n\times n}=\begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n}\\ d_{21} & d_{22} & \cdots & d_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ d_{n1} & d_{n2} & \cdots & d_{nn}\end{bmatrix} \tag{1-5-4}$$

为 G 的联系矩阵。记对角矩阵

$$D(G)=\begin{bmatrix} \sum\limits_i d_{i1} & & & 0\\ & \sum\limits_i d_{i2} & & \\ & & \ddots & \\ 0 & & & \sum\limits_i d_{in}\end{bmatrix}, \tag{1-5-5}$$

而定义

$$Q(G)=D(G)-B(G)=\begin{bmatrix}\sum\limits_{i\neq 1}d_{i1} & -d_{i2} & \cdots & -d_{1n}\\ -d_{i1} & \sum\limits_{i\neq 2}d_{i2} & \cdots & -d_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ -d_{n1} & \cdots & -d_{n,n-1} & \sum\limits_{i\neq n}d_{in}\end{bmatrix}. \tag{1-5-6}$$

以下记 $Q_{k_1\cdots k_r}(G)$ 为 $Q(G)$矩阵划去第 $k_1, k_2, \cdots, k_r$ 行、列后所得的子矩阵，而

$$\Delta_{k_1\cdots k_r}(G)=\|Q_{k_1\cdots k_r}(G)\| \tag{1-5-7}$$

为 $Q_{k_1\cdots k_r}(G)$矩阵的行列式。

另外，我们记

$$d_{i\cdot}=(d_{i1},\cdots,d_{in}),\quad d_{\cdot j}=(d_{\cdot j},\cdots,d_{nj})'$$

为矩阵 $B(G)$的行、列向量，其中矩阵 B' 为 B 的转置矩阵。

引理 4 对上述矩阵 $B(G)$, $D(G)$, $Q(G)$ 有性质如下：

(i) 有向图 $G=\{A, L\}$ 与联系矩阵 $B(G)$在(1-5-3)关系下1-1对应，相互确定。

(ii) 若记 τ 为 $\{1, \cdots, n\}$上的一个置换，$G_\tau=\{A_\tau, L_\tau\}$ 为图 $\{A, L\}$ 的 τ 置换，其中

$$A_\tau=\{t_1, t_2, \cdots, t_n\},\ t_i=s_{\tau^{-1}(i)},$$
$$L_\tau=L. \tag{1-5-8}$$

这时 G_τ 的联系矩阵为

$$B[G_\tau]=[d_{\tau^{-1}(j),\tau^{-1}(i)}]_{n\times n}$$
$$=\begin{bmatrix}d_{\tau^{-1}(1),\tau^{-1}(1)} & d_{\tau^{-1}(1),\tau^{-1}(2)} & \cdots & d_{\tau^{-1}(1),\tau^{-1}(n)}\\ \cdots & \cdots & \cdots & \cdots\\ d_{\tau^{-1}(n),\tau^{-1}(1)} & d_{\tau^{-1}(n),\tau^{-1}(2)} & \cdots & d_{\tau^{-1}(n),\tau^{-1}(n)}\end{bmatrix}. \tag{1-5-9}$$

(iii) $\|Q(G)\|=0$($\|F\|$ 为 F 矩阵的行列式)。

(iv) $\|Q_k(G)\|$ 为向量 $d_{\cdot 1}, \cdots, d_{\cdot n}$ 的线性函数。

证明　(i) 由有向图 $G=\{A, L\}$ 确定 $B(G)$ 见 (1-5-3) 定义；反之，由 $B(G)$ 可确定有向图 G。若记 $A=\{s_1, \cdots, s_n\}$，则定义

$$L=\{(s_j, s_i): d_{ij}=1\},$$

这时 G 与 $B(G)$ 相互唯一确定。

(ii) 在(1-5-8)的定义下，若记 G_τ 的联系矩阵为 $B(G_\tau)=[d'_{ij}]_{n\times n}$，这时

$$d'_{ij}=1\Longleftrightarrow(t_j, t_i)\in L_\tau$$
$$\Longleftrightarrow(s_{\tau^{-1}(j)}, s_{\tau^{-1}(i)})\in L\Longleftrightarrow d_{\tau^{-1}(i),\tau^{-1}(j)}=1,$$

因此(1-5-9)成立。

(iii) 因为 $Q(G)$ 矩阵行的和为零，即

$$\sum_{i=1}^{n} d'_{ij}=0, \text{ 对任何 } j=1, 2, \cdots, n,$$

其中 d'_{ij} 为 $Q(G)$ 矩阵的元，因此 $Q(G)$ 的行列式必为零。

(iv) 由行列式性质即得，因为每个行列式可按其行或列进行展开，因此它们是行或列向量的线性函数，引理得证。

有时我们记

$$\Delta_k(G)=\|Q_k(G)\|=\Delta_k(d_{\cdot 1}, \cdots, d_{\cdot n}),\qquad (1\text{-}5\text{-}10)$$

这时显然有

$$\Delta_k(G_\tau)=\Delta_{\tau^{-1}(k)}(G).\qquad (1\text{-}5\text{-}11)$$

我们把 G_τ 的图看作与 G 相同的图，它们的联系矩阵为相互交换行列的位置。

引理 5　若 $T=\{A, L\}$ 为一反树，则将 A 的点适当排列之后，$B(T)$ 图具有性质：

(i) 若 $i\geqslant j$，则 $d_{ij}=0$。

(ii) $\sum_{i=1}^{n} d_{i1}=0$，$\sum_{i=1}^{n} d_{ij}=1$，$j\neq 1$。

反之，若图 T 的联系矩阵具有性质(i)，(ii)，则 T 为反树图。

证明 若 T 为反树图，则将 T 的全体顶点按层次排列为

$$\{s_1, s_2, \cdots, s_{t_1}, s_{t_1+1}, \cdots, s_{t_2}, \cdots, s_{t_k}\},$$

$t_0=1$，s_1 为反树 T 的零层顶点，而

$$\{s_{t_j+1}, \cdots, s_{t_{j+1}}\} \ (j=0, 1, \cdots, k-1)$$

为反树 T 的 $j+1$ 层顶点，这时对任何弧 $(s_j, s_i) \in L$，若 s_i 在 T 的 r 层，则 s_j 必在 $r+1$ 层，因此必有 $j>i$。故性质(i)必成立。

关于性质(ii)由反树的定义即得，因为这时 s_1 点没有出弧，而其余的点有且只有一条出弧，因此性质(ii)成立。

反之，若 $B(T)$ 具有性质(i)(ii)，这时在本节定义 1 中反树图的条件(i)，(ii)，可由引理 4 即得。再证明本节定义 1 中条件(iii)成立即可。

设 s_{j_0} 为 T 的任一顶点，$j_0 \neq 1$。这时总有一个 $j_1<j_0$，使 $d_{j_1 j_0}=1$。此即 s_{j_1} 为 s_{j_0} 的后继，若 $j_1=1$，则 s_{j_0} 由 (s_{j_0}, s_{j_1}) 到达 s_1；若 $j_1>1$，则必有 $j_2<j_1$，使 $d_{j_2 j_1}=1$。同样 s_{j_2} 为 s_{j_1} 的后继，如 $j_2=\varnothing$，则 s_{j_0} 由路 $(s_{j_0}, s_{j_1}, s_{j_2})$ 到达 s_1；如 $j_2>1$，则可同样构造 j_3，t_{j_3}。如此继续，我们得到一列

$$j_0>j_1>j_2>\cdots\geqslant 1,$$

因为 j_0 是个有限数，因此以上的 j_i 只能构造有限次，最终得到 $j_k=1$，这时 s_{j_0} 由路

$$(s_{j_0}, s_{j_1}, s_{j_2}, \cdots, s_{j_{k-1}}, s_{j_k}=s_1)$$

到达 s_1，因此 T 必为反树图。引理得证。

引理 6 $B(G)$ 为 G 的联系矩阵，且 $d_1=0$，$d_2=\cdots=d_n=1$，则 G 为以 s_1 为根的反树的充要条件为 $\Delta_1(G)\neq 0$，这时必有 $\Delta_1(G)=1$，其中

$$d_j=\sum_{i=1}^{n} d_{ij}, \quad n=\|A\|.$$

证明 条件 $d_1=0$，$d_2=\cdots=d_n=1$ 与本节反树的定义 1 的

(i),(ii) 等价，其中 s_1 为根，因此我们只要证明定义 1 的条件(iii)与 $\Delta_1(G)\neq 0$ 等价就可。

为证明上述条件的等价性，我们讨论矩阵 $Q_{i_1\cdots i_r}(G)$ 为 $Q(G)$ 划去 i_1，…，i_r 行、列而得的子矩阵，这时 $Q_{i_1\cdots i_r}(G)$的列有以下两种类型的向量构成，即

$$d_j^{(1)}=(\overbrace{0\cdots 0}^{j-1},-1,\overbrace{0\cdots 0}^{n-r-j},1,0,\cdots 0)', \tag{1-5-12}$$

$$d_j^{(1)}=(\overbrace{0,\cdots,0}^{j-1},1,\overbrace{0,\cdots 0}^{n-r-j})'. \tag{1-5-12a}$$

在(1-5-12)的向量类型中，-1 的元也可在 $+1$ 的后边。以下我们称(1-5-12a)的列向量为Ⅱ-型向量，(1-5-12)的列向量为Ⅰ-型向量。

现在讨论矩阵 $Q_{i_1\cdots i_r}(G)$，先取 $i_1=1$，若定义 1 中条件(iii)成立，则

$$(d_{11},d_{12},\cdots,d_{1n})\neq(\overbrace{0,0,\cdots,0}^{n}),$$

否则任何 $s_i(i=2,3,\cdots,n)$都不能到达 s_1，因此在 $Q_1(G)$ 中至少存在一个Ⅱ-型向量 $d_j^{(1)}$ 而取 i_2 为 $d_j^{(1)}$ 所在的列，即 $Q_{1i_2}(G)$ 在 $Q_1(G)$ 中划去第 j 行、列，其中 j 是使 $d_j^{(1)}$ 为Ⅱ-型向量。

这样，重复上述步骤，在 $Q_{1i_2}(G)$ 中寻找Ⅱ-型向量 $d_j^{(2)}$，如存在，则划去 $Q_{1i_2}(G)$ 中的的第 j 行、列，得到 $Q_{1i_2i_3}$，其中 j 是使 $d_j^{(2)}$ 为Ⅱ-型向量的下标。如此继续，如定义 1 的条件(iii)满足，经过若干次运算，最终总可将 $Q_{1i_1\cdots i_k}(G)$ 矩阵变为只有Ⅱ-型向量的矩阵，即为幺矩阵，这时

$$\Delta_1(G)=\Delta_{1i_1\cdots i_k}(G)=1$$

成立。

如果定义 1 的条件(iii)不成立，经过上述若干次运算之后，最终将 $Q_{1i_1\cdots i_k}(G)$化成只有Ⅰ-型列向量的矩阵，这时 $Q_{1i_1\cdots i_k}(G)$

在 $Q(G)$ 所在的行、列标号为不可到达 x_1 的点的标号。因为 $Q_{1i_2\cdots i_k}(G)$ 只有 I -型的列向量，因此将 $Q_{1i_2\cdots i_k}(G)$ 的所有行相加必为零向量，所以

$$\Delta_1(G)=\Delta_{1i_2\cdots i_k}(G)=0。$$

由此引理得证。

引理 6 的条件还可放宽为

引理 7 如 $G=\{A, L\}$ 为一个无环图，$\|A\|=\|L\|+1$，则 G 为以 s_1 为根的反树图的充要条件为 $\Delta_1(G)\neq 0$ 或 $\Delta_1(G)=1$。

证明 我们将 G 图的顶点 s_i 按其出弧数的大小次序排列，记

$$d_{\cdot j}=\sum_{i=1}^{n} d_{ij} \quad (n=\|A\|)$$

为 s_j 的出弧数，且 $d_1\leqslant d_2\leqslant\cdots\leqslant d_n$，因为

$$\sum_{j=1}^{n} d_{\cdot j}=\|L\|=\|A\|-1=n-1,$$

所以 $d_1=0$。

若 G 为反树图，则 $d_2=d_3=\cdots=d_n=1$，这时将 $s_2, \cdots, s_n$ 按 G 图的层次排列，对任何 $i\geqslant j$，$d_{ij}=0$，因此

$$Q(G)=\begin{bmatrix} 0 & & & \\ 0 & 1 & & D \\ 0 & 0 & 1 & \\ \cdots & \cdots & \cdots & \ddots \\ & & & \ddots \\ 0 & 0 & \cdots & 0 \quad 1 \end{bmatrix}, \tag{1-5-13}$$

其中 D 为由 0，1 构成三角形，则

$$Q_1(G)=\begin{bmatrix} 1 & & & \\ 0 & 1 & & D' \\ \vdots & \ddots & \ddots & \\ 0 & \cdots & 0 & 1 \end{bmatrix},$$

其中 D' 为由 D 划去第 1 行和第 1 列后所得的三角形。因此 $\Delta_1(G)=1$ 必成立。

反之，若 $\Delta_1(G)\neq 0$，则必有 $d_2=d_3=\cdots=d_n=1$ 成立，否则就有 $i\neq 1$，使 $d_i=0$，则 $\Delta_1(G)=0$。这样由本节引理 6 即可得到 G 为以 a_1 为根的反树，则引理 7 得证。

5.3　反图树的计数问题

反树图的计数问题，是对已给的图 $G=\{A, L\}$ 求 G 的极大反树子图 $T=\{A, L'\}$ 的个数问题。若我们记 $A=\{s_1, \cdots, s_n\}$，而

$$\tilde{T}(G)=\{T=\{A, L'\}: L'\subset L \text{为反树图}\}, \quad (1\text{-}5\text{-}14)$$

即为 G 的全体极大反树子图。而记

$$\tilde{T}_1(G)=\{T=\{A, L'\}\subset\tilde{T}(G), \text{且以 } s_1 \text{ 为根}\}。 \quad (1\text{-}5\text{-}15)$$

这时有

定理 1　由(1-5-15)，有

$$\|\tilde{T}_1(G)\|=\Delta_1(G)。 \quad (1\text{-}5\text{-}16)$$

成立，即 G 中以 s_1 为根的极大反树子图的个数正好等于行列式 $\Delta_1(G)$ 的值。

证明　先假定 G 为无环图，定义

$$c_k^{(n)}=(e_{k1}, e_{k2}, \cdots, e_{kn}),$$

其中 $e_{kk}=1$，其余分量为 0。另外记

$$\alpha_i=\{j: (s_i, s_j)\in L\}=\{j: d_{ji}=1\}。$$

这时有

$$d_{\cdot j}=\sum_{i\subset\alpha_j} e_i^{(n)},\ j=1, 2, \cdots, n,$$

成立。因为

$$\Delta_1(G)=\Delta_1(d_{\cdot 2},\cdots,d_{\cdot n})$$

是 $d_{\cdot 2},\cdots,d_{\cdot n}$ 的线性函数，因此

$$\Delta_1(G)=\sum_{i_2\in\alpha_2}\cdots\sum_{i_n\in\alpha_n}\Delta_1(e_{i_2}^{(n)},\cdots,e_{i_n}^{(n)}). \qquad (1\text{-}5\text{-}17)$$

如我们定义

$$G(i_2,\cdots,i_n)=\{A,L(i_2,\cdots,i_n)\}$$

为 G 的子图，其中

$$L(i_2,\cdots,i_n)=\{(s_2,s_{i_2}),(s_3,s_{i_3}),\cdots,(s_n,s_{\cdot i_n})\}\subset L,$$

因为对任何 $j=2,3,\cdots,n$，$i_j\in\alpha_j$。这时图 $G(i_2,\cdots,i_n)$满足本节引理 7 的条件

$$\|L\|=\|A\|-1=n-1,$$

因此

$$\Delta_1[G(i_2,\cdots,i_n)]=\begin{cases}1,\text{若 } G(i_2,\cdots,i_n)\text{是以 } s_1 \text{ 为根的反树},\\ 0,\text{否则}.\end{cases}$$

由(1-5-17)即可证得(1-5-16)成立。

如 G 中有环，因为任何反树都不能有环，这时可除去 G 中所有的环，得图 G'，这时

$$\|\tilde{T}_1(G)\|=\|\tilde{T}_1(G')\|.$$

另一方面，又有

$$D(G')-B(G')=D(G)-B(G)$$

成立，因此有

$$\Delta_1(G)=\Delta_1(G')=\|\tilde{T}_1(G')\|=\|\tilde{T}_1(G)\|$$

成立，此即(1-5-16)成立，定理得证。

定理 2 在 $G_n(q)$图中，对任何 $n\geqslant 1$，$q\geqslant 2$，有

$$\Delta_1[G_n(q)]=q^{q^n-(n+1)} \qquad (1\text{-}5\text{-}18)$$

成立，其中取 $s_1=(0,0,\cdots,0)$。

证明 我们将 $F_o^{(n)}$ 中的元按

$$i(a_0, a_1, \cdots, a_{n-1}) \overset{*}{=} a_0 + a_1 q + \cdots + a_{n-1} q^{n-1} \quad (1\text{-}5\text{-}19)$$

的次序排列，(1-5-19)式中的加、乘运算均为在实数中的运算，且称 $i(a_0, \cdots, a_{n-1})$ 的值为向量 $(a_0, \cdots, a_{n-1})$ 的编号，这时 $G_n(q)$ 的联系矩阵为

$$B[G_n(q)] = \left.\begin{bmatrix} I_n \\ I_n \\ \vdots \\ I_n \end{bmatrix}\right\} q \text{ 个}, \quad (1\text{-}5\text{-}20)$$

其中

$$I_n = \left.\begin{bmatrix} \overbrace{1\ 1 \cdots 1}^{q\text{个}} & & & 0 \\ & 1\ 1 \cdots 1 & & \\ & & \ddots & \\ 0 & & & 1\ 1 \cdots 1 \end{bmatrix}\right\} q^{n-1} \text{ 行} \quad (1\text{-}5\text{-}21)$$

这时 $B[G_n(q)]$ 为 $q^n \times q^n$ 矩阵，而 I_n 为 $q^{n-1} \times q^n$ 矩阵，这时可将 I_n 写成

$$I_n = \begin{bmatrix} I_{n-1} & O_{n-1} & \cdots & O_{n-1} \\ O_{n-1} & I_{n-1} & \cdots & O_{n-1} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ Q_{n-1} & O_{n-1} & \cdots & I_{n-1} \end{bmatrix},$$

其中 I_{n-1} 与 I_n 定义相同，O_{n-1} 为 $q^{n-2} \times q^{n-1}$ 阶零矩阵。如定义

$$B_1 = \begin{bmatrix} I_{n-1} \\ O_{n-1} \\ \vdots \\ O_{n-1} \end{bmatrix}, B_2 = \begin{bmatrix} O_{n-1} \\ I_{n-1} \\ \vdots \\ O_{n-1} \end{bmatrix}, \cdots, B_q = \begin{bmatrix} O_{n-1} \\ O_{n-1} \\ \vdots \\ I_{n-1} \end{bmatrix},$$

这时

$$B[G_n(q)]=\left.\begin{bmatrix} B_1 & B_2 & \cdots & B_q \\ B_1 & B_2 & \cdots & B_q \\ \cdots\cdots & & & \\ B_1 & B_2 & \cdots & B_q \end{bmatrix}\right\} q\text{ 个} \quad (1\text{-}5\text{-}22)$$

而

$$Q[G_n(q)]=\begin{bmatrix} E-B_1 & -B_2 & \cdots & -B_q \\ -B_1 & E-B_2 & \cdots & -B_q \\ \cdots\cdots & & & \\ -B_1 & -B_2 & \cdots & E-B_q \end{bmatrix}$$

$$=\begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_q \end{bmatrix}, \quad (1\text{-}5\text{-}23)$$

其中 $E=q\cdot E_{n-1}$，E_{n-1} 为 $q^{n-1}\times q^{n-1}$ 阶幺矩阵，H_i 为 $Q[G_n(q)]$ 中的分块行矩阵。

若在 $Q[G_n(q)]$ 的分块行矩阵(1-5-21)中，将第 i 行减第 q 行，得矩阵为

$$Q'[G_n(q)]=\begin{bmatrix} E & O & \cdots & O & -E \\ O & E & \cdots & O & -E \\ \cdots\cdots & & & & \\ O & O & \cdots & E & -E \\ -B_1, & -B_2, & \cdots, & -B_{q-1} & E-B_q \end{bmatrix}$$

$$=[c_1, h_1, c_2, h_2, \cdots c_q, h_q], \quad (1\text{-}5\text{-}24)$$

其中 O 为 $q^{n-1}\times q^{n-1}$ 阶零矩阵，c_i，h_i 为 $Q'[G_n(q)]$ 的分块列矩阵，其中 c_i 为 $q^n\times 1$ 阶矩阵，h_i 为 $q^n\times(q^{n-1}-1)$ 阶矩阵。这时将 c_2，$\cdots c_{q-1}$ 矩阵加到 c_q 列矩阵上，h_1，h_2，$\cdots$，h_{q-1} 矩阵加到 h_q 矩阵上，则 $Q'[G_n(q)]$ 矩阵变为

$$Q''[G_n(q)]=\begin{bmatrix} E & O & \cdots & O & R \\ O & E & \cdots & O & O \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ O & O & \cdots & E & O \\ -B_1 & -B_2 & \cdots & -B_{q-1} & P \end{bmatrix}, \quad (1\text{-}5\text{-}25)$$

其中 R，P 均为 $q^{n-1}\times q^{n-1}$ 阶矩阵，

$$P=E-B_1-\cdots-B_q-q^{-1}R,$$

而

$$R=\begin{bmatrix} -q & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

这时

$$\Delta_1[G_n(q)]=\|Q_1''[G_n(q)]\|=q^{(qn-q^{n-1}-1)}\|P\| \quad (1\text{-}5\text{-}26)$$

其中 Q_1'' 为 Q'' 划去第 1 行第 1 列后的矩阵，关系式(1-5-26)由行列式运算的性质而得。

如上所记，E_{n-1} 为 $q^{n-1}\times q^{n-1}$ 阶幺矩阵，$E=q\cdot E_{n-1}$，这时

$$Q[G_{n-1}(q)]=E-\begin{bmatrix} I_{n-1} \\ \vdots \\ I_{n-1} \end{bmatrix}=E-B_1-\cdots-B_q, \quad (1\text{-}5\text{-}27)$$

如将 P 矩阵的第 2，3，…，q^{n-1} 行加到第 1 行上，则 P 矩阵的第 1 行变为(1，0，0，…，0)，因此由(1-2-27)得

$$\|P\|=\Delta_1[G_{n-1}(q)].$$

这时由(1-5-26)可得

$$\Delta_1[G_n(q)]=q^{qn-q^{n-1}-1}\Delta_1[G_{n-1}(q)]. \quad (1\text{-}5\text{-}28)$$

另一方面，当 $n=1$ 时

$$B[G_1(q)]=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}_{q\times q},$$

$$Q[G_1(q)]=\begin{bmatrix} q-1 & -1 & \cdots & -1 \\ -1 & q-1 & \cdots & -1 \\ \cdots & \cdots & \cdots & \cdots \\ -1 & -1 & \cdots & q-1 \end{bmatrix}_{q\times q},$$

则由矩阵的运算可得

$$A_1[G_1(q)]\overset{*}{=}\left\|\begin{matrix} q-1 & -1 & \cdots & -1 \\ -1 & q-1 & \cdots & -1 \\ \cdots & \cdots & \cdots & \cdots \\ -1 & -1 & \cdots & q-1 \end{matrix}\right\|_{(q-1)\times(q-1)}$$

$$\overset{*}{=}q^{q-2}, \qquad (1\text{-}5\text{-}29)$$

从(1-5-29)和(1-5-28)可得(1-5-18)成立,从而定理得证。

§6 M-序列的构造与计数问题

本节在主要介绍利用反树图的构造与计数理论对 $G_n(q)$中的全体 M-序列进行构造与计数。

6.1 关于倍图中的极大圈性质

利用倍图中的极大圈性质是 M-序构造中的重要一环，因此我们先介绍这一性质。

定义 设 $G=\{A, L\}$ 为一个圈，称 $G^*=\{A^*, L^*\}$ 为 G 的一个倍图,如

(i) G 中的弧为 G^* 的顶点,即 $A^*=L$。

(ii) L^* 为 G 中两条相连的弧。

引理 (i) 如 G 为一个 q 图，则 $\|A^*\|\overset{*}{=}q\cdot\|A\|$。

(ii) $G_{n+1}(q)$图为 $G_n(q)$的倍图。

(iii) 若

$$W=\{s_0, s_1, \cdots, s_k\}=\{S_0, S_1, \cdots, S_k\} \quad (1\text{-}6\text{-}1)$$

为 G 的一回路(其中 $S_i=(s_i, s_{i+1})$, $i=0, 1, \cdots, k$, $s_{k+1}=s_0$),则

$$W^*=\{s_0^*, s_1^*, \cdots, s_k^*\}=\{S_0^*, S_1^*, \cdots, S_k^*\} \quad (1\text{-}6\text{-}2)$$

为 G^* 中的一条回路,其中 $s_i^*=S_i$,而

$$S_i^*=(S_i, S_{i+1}), \ i=b, 1, \cdots, k, S_{k+1}=S_0.$$

这些性质由倍图、$G_n(q)$ 图及回路的定义即得. 以下我们称 W^* 为 W 的扩张。

关于倍图中回路的基本性质为

定理 1　若 G^* 为 G 的倍图,则 W 为 G 的一条完备回路的充要条件是它的扩张 W^* 为 G^* 中的极大圈。

证明　充分性。若 W 为 G 中的完备回路，则在(1-6-1) 中，$\{S_0, S_1, \cdots, S_k\}$为 G 的全体弧 L，因为 W^* 是 W 的扩张，因此 W^* 为 G^* 的回路且过 G^* 的全体点的初等回路，即 W^* 为 G^* 的极大圈。

必要性。若 W^* 为 G^* 的极大圈，则在(1-6-2)中，$\{s_0^*, s_1^*, \cdots, s_k^*\}=\{S_0, S_1, \cdots, S_k\}$ 为 G 的全体弧。记 $S_i=(s_i, s_{i+1})$，则由

$$S_{k+1}=S_0 \Rightarrow (s_{k+1}, \ s_{k+2})=(s_0, s_1) \Rightarrow s_{k+1}=s_0,$$

知 $W=\{s_0, s, \cdots, s_k\}=\{S_0, S_1, \cdots, S_k\}$为 G 的回路,且是 G 单回路,过 G 的全体弧,因此 W 为 G 的完备回路。定理得证。

这样，我们可将 G^* 中的极大圈与 G 中的完备回路进行等价讨论，即有了 G^* 中的极大圈，就有 G 中的完备回路。反之，有了 G 中的完备回路,就有 G^* 中的极大圈。对此,以后就不再一一说明了。

6.2　过反树 T 的完备回路

以下我们均在 $G_n(q)$图中讨论，因为 $G_{n+1}(q)$ 为 $G_n(q)$ 的倍

图，因此 $G_n(q)$中的完备回路即 $G_{n+1}(q)$中的极大圈。以下我们称 $G_n(q)$中的极大圈为 $M_n(q)$-序列，且记

$$k_n = k_n(q) = q^n - 1。$$

若 W 为(1-6-1)定义的 $G_n(q)$中的完备回路，这时 $k = k_{n+1} = q^{n+1} - 1$，且称 s_0 为 W 的起点，$(s_0, s_1) = S_0$ 为 W 的起弧。在单回路中，起点与起弧均可任意选取，一旦起弧选定，单回路中各弧的次序就排定了。

若 W 是 $G_n(q)$ 的完备回路，起弧 S_0 选定，这时对每个状态

$$s = (a_0, a_1, \cdots, a_{n-1}) \in G_q^{(n)},$$

在 W 中有 q 条出弧，且按一定的次序排列，以下记

$$I(s) = \{(s, a_n(s, i)), i = 1, 2, \cdots, q\} \qquad (1\text{-}6\text{-}3)$$

为 $s \in F_q^{(n)}$ 的出弧在 (W, S_0)中的排列次序，其中 $a_n(s, i) \in F_q$。称 $I(s) = I(s, W, S_0)$为 s 出弧在(W, S_0)中的编号。而称

$$I(W, S_0) = \{Q(s, W, S_0) \cdot s \in F_q^{(n)}\} \qquad (1\text{-}6\text{-}4)$$

为完备回路(W, S_0)的编号集。以下记

$$T(W, S_0) = \{A, I(W, S_0)\} \qquad (1\text{-}6\text{-}5)$$

为过 W 的反树图，其中 $A = F_q^{(n)}$，而

$$T(W, S_0) = \{(s', a_n(s, q)) : s' \in F_{q,0}^{(n)}\}, \qquad (1\text{-}6\text{-}6)$$

$F_{q,0}^{(n)} = F_q^{(n)} - \{s_0\}$，即 $I(W, s_0)$为 W 在 s_0 点的最后一条出弧。这时有

定理 2 对任何 $G_n(q)$中的完备回路 W，由(1-6-5)、(1-6-6)确定的 $T = T(W, S_0)$为 $G_n(q)$的极大反树子图。

证明 该定理证明分以下几点进行：

(i) 由 $T = T(W, S_0)$的定义(1-6-5)知，T 的顶点集合 $A = F_q^{(n)}$，因此具有极大性，所以只要证明它的反树性质即可。

(ii) 由(1-6-6)的 $L(W, S_0)$ 定义知，对任何 $s \neq s_0 \in F_q^{(n)}$，有且总有一条出弧：$(s, a_n(s, q))$，且 s_0 点没有出弧，因此 §5 定义 1 中反树的的条件(i)，(ii)成立。

(iii) 在图$T(W,S_0)$中必没有圈，如$T(W,S_0)$中含一个圈C，那么$s_0\notin C$，因为s_0在T中没有出弧，因此s_0不可能在C中。

另一方面，s_0也是W的终点，任何点必可到达s_0，因此C圈中的点也必到达s_0，这时总有一个$s_1\in C$，使W在s_1点离开C，且这条弧的编号一定在圈C中弧的编号之后，这就与T，C的定义矛盾，因此在图T中不能有圈，又由§5引理2知，图T必为为反树图，定理得证。

如果在图$G_n(q)$中引出一条路

$$W_k=\{s_0, s_1, \cdots, s_k\}=\{S_0, S_1, \cdots, S_{k-1}\}, \quad (1\text{-}6\text{-}7)$$

其中$S_i=(s_i, s_{i+1})$，这时我们称W_k从s_0出发到达s_k，经过(或走过)点$s_0, s_1, \cdots, s_{k-1}$，或弧$S_0, S_1, \cdots, S_{k-1}$。若弧$S\notin\{S_0, \cdots, S_{k-1}\}$，则称$W_k$未经过$S$。同样又称$W_k$为路$W_{k-1}$沿弧$S_{k-1}$的延伸。同样可称$s_k$为$W_{k-1}$的一个延伸点。

定理3　如$T=\{A, L\}$为$G_n(q)$的极大部分反树图，s_0为根。又如$S_0=(s_0, s_1)$为$G_n(q)$的弧(以s_0为先导)，这时在$G_n(q)$中总有一条完备回路W，使$T(W, S_0)=T$。

该回路W可按以下原则来选取：

(1) W从反树T的根s_0出发，首先到达本节定理2中的s_1，得到路

$$W_1=\{s_0, s_1\}=\{S_0\},$$

并继续往下延伸。

(2) 若所延伸的路为(1-6-7)的W_k，且在所到达的s_k点上有若干条出弧为W_k没有走过，则可从这些没有走过的出弧中选出一条继续往下延伸得到W_{k+1}，且在这些没有走过的出弧中总是先取非反树图T中的弧来走，最后才走反树图T上的弧。

(3) 对W_k中已走过的弧不再重复，若W_k到达s_k时s_k的全部出弧都已走过，这时W_k就停止在s_k处，不再继续延伸。

这样得到的 W_k 即为所求的完备回路。

证明 首先按上述步骤来取的路起弧为 $S_0=(s_0, s_1)$，以下只要证所得路必为完备回路，且 $T(W, S_0)=T$ 成立。对此分以下几点来证：

(i) 在 W_k 中对任何 $s_k \neq s_0$ 的点，若有一条入弧到达 s_k，则必有一条出弧离开 s_k，因为 W_k 中所取的弧不重复，且每个 $s \in F_q^{(n)}$ 点的出入弧数目相等。因此按上述(1)—(3)的步骤取的 W_k 最终必停留在 $s_{k_0}=s_0$ 上。这时 W_{k_0} 为回路，且为单回路。

(ii) 为证 W_{k_0} 的完备性，我们只要证 $G_n(q)$ 的任何顶点 s 的出弧都在 W_{k_0} 上。为此用归纳法证明。

(a) 对 T 的零层顶点 s_0，周长 W_{k_0} 最后停止在 s_0 上，因此 s_0 的全体出弧必在 W_{k_0} 上。

(b) 设 T 的 $k-1$ 层顶点的全体出弧都在 W_{k_0} 上，证明 T 的第 k 层顶点的全体出弧也都在 W_{k_0} 上。

对此可用反证法证明。若有一个 s 为 T 的 k 层顶点，有一条出弧 $(s, t) \notin W_{k_0}$，这时必有一个 t'，使 (s, t') 为 T 的弧，且 $(s, t') \notin W_{k_0}$。因此 t' 为 T 的 $k-1$ 层顶点，这时 t' 的全体出弧都在 W_{k_0} 上，因为 $k \geqslant 1$，所以 $t' \neq s_0$，由 W_{k_0} 的单回路性质知，t' 的全体入弧都必在 W_{k_0} 上，这与 t' 的选取条件矛盾，因此 t' 不存在。命题得证。

由此已证得 W_{k_0} 为一完备回路且记之为 W。

(iii) 由条件 $T(W, S_0)=T$ 为 $W=W_{k_0}$ 的取法原则即得，因此 $W=W_{k_0}$ 即为所求。定理得证。

从以上讨论我们即可得到 $G_{n+1}(q)$ 上的全体 $M_{n+1}(q)$-序列的构造过程，它们是：

M_0-Ⅰ 在 $G_n(q)$ 上选取极大部分反树图 T 及起始弧 $S_0=(s_0, s_1)$，其中 s_0 为 T 的根，s_1 为任取且使 (s_0, s_1) 为 $G_n(q)$ 的弧。

M_0-Ⅱ 按本章 §6 定理 3 的骤步构造 $G_n(q)$ 中的完备回路

W，使 $T(W, S_0)=T$ 成立。

M_0-Ⅲ 将 W 扩张为 W^*，则 W^* 必为 $G_n(q)$ 的 M-序列(即 $M_{n+1}(q)$-序列)。

我们以后还要将这些步骤具体化，使之成为一定的密钥参数空间与一定的算法，在此不再详述。

6.3 关于 $M_n(q)$-序列的计数公式

由本章 §5及 §6 的讨论我们可以得到关于 $M_n(q)$-序列的计数公式。为此记 T 为 $G_n(q)$中的极大部分反树图，$S_0=(s_0, s_1)$，s_0 为 T 的根，(s_0, s_1) 为 $G_n(q)$的弧。这时定义：

$$\widetilde{W}_n(T, S_0)=\{G_n(q)\text{ 中的全体完备回路，以 }S_0\text{ 为起始弧，}T(W, S_0)=T\}。\quad(1\text{-}6\text{-}8)$$

$$\widetilde{W}(S_0; n, q)=\{G_n(q)\text{ 中的全体完备回路，以 }S_0\text{ 为起弧}\}。\quad(1\text{-}6\text{-}9)$$

$$\widetilde{M}(S_0; n+1, q)=\{G_{n+1}(q)\text{中的全体 }M\text{-序列，以 }S_0\in F_q^{(n+1)}\text{ 为起点}\}。\quad(1\text{-}6\text{-}10)$$

它们相应的计数定义为

$$\begin{cases} W_n(T, S_0)=\|\widetilde{W}_n(T, S_0)\|, \\ W(S_0; n, q)=\|\widetilde{W}(S_0; n, q)\|, \\ M(S_0; n+1, q)=\|\widetilde{M}(S_0; n+1, q)\|。 \end{cases}\quad(1\text{-}6\text{-}11)$$

这时显然有

$$W(S_0; n, q)=M(S_0; n+1, q)\quad(1\text{-}6\text{-}12)$$

成立，我们现在介绍其他的计数公式。

定理 4 对(1-6-11)的计数定义有

$$W(T, S_0)\overset{*}{=}[((q-1)!\,]^{q^n},\quad(1\text{-}6\text{-}13)$$

及

$$W(S_0; n, q)\overset{*}{=}(q!\,)^{q^n}\cdot q^{-(n+1)},\quad(1\text{-}6\text{-}14)$$

在(1-6-13)、(1-6-14)中的运算均为实数中的运算。

证明 对定理的(1-6-13)、(1-6-14)式分以下几步证明。

(i) 若 T、S_0 已给定，则由完备回路 W 的构造过程，即本节定理 2 的步骤知道，W 在 $F_q^{(n)}$ 的每个顶点 s_0，除了 T 中的弧或 $S_0=(s_0, s_1)$ 选取次序固定外，其余 $q-1$ 个任取，因此每个 s 点出弧次序的选择有 $(q-1)!$ 个，全体 $F_q^{(n)}$ 点的出弧次序排列有

$$[(q-1)!]^{q^n}$$

种，且每个不同的次序选择均可得到不同的完备回路，所以公式(1-6-13)成立。

(ii) 为证明公式(1-6-14)，我们先证

$$\widetilde{W}_n(T, S_0),\ T\in\widetilde{T}_n(s_0) \qquad (1\text{-}6\text{-}15)$$

为 $\widetilde{W}(S_0, n, q)$ 的一个分割，其中 $\widetilde{T}_n(s_0)$ 为 $G_n(q)$ 中全体以 s_0 为根的反树图，因此这时有：

(a) 对任何 $T\neq T'\in\widetilde{T}_n(s_0)$，必有

$$\widetilde{W}_n(T, S_0)\cap\widetilde{W}_n(T', S_0)=\varnothing(\text{空集}). \qquad (1\text{-}6\text{-}16)$$

(b) 对 $G_n(q)$ 中的任何完备回路 W，总有 $T\in\widetilde{T}_n(s_0)$，使 $W\in\widetilde{W}_n(T, S_0)$。

关于性质(a)，由 $\widetilde{W}_n(T, S_0)$ 即可得到。因为 $T\neq T'$，则由 T 及 T' 构造的完备回路均不相同，因此(1-6-16)必成立。另外，对任何 $G_n(q)$ 中的完备回路 W，可以任选一弧为起始弧，我们取为 $S_0=(s_0, s_1)$，根据本节定理 1，由 W，S_0 确定的 $T'(W, S_0)=T$ 为反树图，因此性质(b)必成立，这时(1-6-15)的集合类为 $\widetilde{W}(S_0, n, q)$ 的分割类。

(iii) 由证明(ii)的性质及(1-6-13)与(1-5-18)即得

$$W(S_0; n, q)\overset{*}{=}\sum_{T\in\widetilde{T}_n(s_0)}W_n(T, S_0)\overset{*}{=}[(q-1)!]^{q^n}\cdot\|\widetilde{T}_n(s_0)\|$$

$$\overset{*}{=}[(q-1)!]^{q^n}\cdot q^{q^n-(n+1)}\overset{*}{=}(q!)^{q^n}\cdot q^{-(n+1)},$$

则(1-6-14)成立，定理得证。

定理 4 称为 $M_n(q)$-序列的计数定理。

第 二 章

非线性复杂度的综合分析

本章重点讨论周期序列（或 q 值向量）的非线性复杂度问题，其中包括非线性复杂度的组合计算公式，非线性反馈移位寄存器的综合解与剩余度问题，同时讨论了线性移位寄存器综合解的组合递推计算算法与剩余度问题。有关这些问题的内容与意义，我们将在下文中详述。

§1 非线性复杂度的递推算法

1.1 非线性复杂度的递推计算问题

在上一章 §2 中，我们已介绍了一般 q 值向量 $a^{(p)}$ 的线性复杂度与它的 Berlekamp-Massey 算法，同时指出了它们在序列密码体制中的作用与地位，给出了线性复杂度低的序列加密体制必不可取的结论。另一方面，由于序列加密体制的非线性化趋势，线性复杂度已不再是序列加密体制优劣判别的唯一标志，这是因为在非线性序列中，线性复杂度高的体制未必一定安全，我们还可找到其他非线性的攻击方法，因此非线性复杂度的指标在密码学中的作用也很重要。

正如上一章 §2 中所指出的那样，线性复杂在密码学中的重要性不仅在于它定义本身的含意，还在于 B-M 算法的给定及相应的剩余度性质，正由于这些算法与性质的给定，才能使对线性复杂度低的序列的攻击成为可能。因此，要使非线性复杂度在密码学中发挥作用，我们必需找到相应算法的关于非线性复杂度的递推算法，本节的目的就是讨论这个问题。

1.2 非线性复杂度的一个组合计算公式

在上一章 §1 中我们已给出了一个向量

$$a^{(p)}=(a_0, a_1, \cdots, a_{p-1}), a_i \in F_q$$

的非线性复杂度的定义公式，即(1-1-22)中定义的 $C_N(a^{(p)})$，现在进一步讨论 $C_N(a^{(p)})$的组合表示。如前所记，对固定的向量 $a^{(p)}$，记

$$a(i, j)=(a_i, a_{i+1}, \cdots, a_j), 0 \leqslant i \leqslant j \leqslant p-1$$

为 $a^{(p)}$ 在(i, j)上的向量段，而

$$\begin{aligned} S_t^n &= a(t-n, t-1) \\ &= (a_{t-n}, a_{t-n+1}, \cdots, a_{t-1}) \end{aligned} \tag{2-1-1}$$

为 $a^{(p)}$ 的一个状态向量，$n \leqslant t < p-1$。这时定义

$$A_b^{(n)}(a^{(p)})=\{S_t^{(n)}: a_t=b, n \leqslant t < p-1\},$$

称

$$A_F^{(n)}(a^{(p)})=\{A_b^{(n)}(a^{(p)}): b \in F_q\} \tag{2-1-2}$$

为 $a^{(p)}$ 的组合分解。

引理 $f(x^{(n)})$为 $a^{(p)}$ 的生成函数的充要条件为

$$A_b[f(x^{(n)})] \supset A_b^{(n)}(a^{(p)}) \tag{2-1-3}$$

对任何 $b \in F_q$ 成立。

该引理由生成函数的定义及 $A_b[f(x^{(n)})]$与 $A_b^{(n)}(a^{(p)})$的定义即得。关于 $f(x^{(n)})$生成 $a^{(p)}$ 的定义见第一章 §1 中定义 3。

定理 1 关于(1-1-22)定义的非线性复杂度 $C_N(a^{(p)})$ 有公式

$$C_N(a^{(p)}) \overset{*}{=} \min\{n: \bigcup_{\substack{(b,b'):\\ b\neq b'\in F_q}} [A_b^{(n)}(a^{(p)}) \cap A_{b'}^{(n)}(a^{(p)})] = \varnothing\} \tag{2-1-4}$$

成立，我们称公式(2-1-4)为非线性复杂度的组合表示。

证明　记(2-1-4)右边的值为$C'_N(a^{(p)})$，若有一个函数$f(x^{(n)})$生成$a^{(p)}$，则由本节引理知关系式(2-1-3)对任何$b\in F_q$成立，因为

$$A_F[f(x^{(n)})] = \{A_b[f(x^{(n)})], b\in F_q\}$$

为$F_q^{(n)}$的一组分割，因此

$$A_b^{(n)}(a^{(p)}), b\in F_q$$

必互不相交，则有

$$\bigcup_{\substack{(b,b'):\\ b\neq b'\in F_q}} [A_b^{(n)}(a^{(p)}) \cap A_{b'}^{(n)}(a^{(p)})] = \varnothing, \tag{2-1-5}$$

成立，故必有$C_N(a^{(p)}) \leqslant C'_N(a^{(p)})$成立。反之，如(2-1-5)成立，则$A_b^{(n)}(a^{(p)})$互不相交，这时取

$$B_b^{(n)}(a^{(p)}) = \begin{cases} A_b^{(n)}(a^{(p)}), & \text{若 } b\neq 0, \\ F_q^{(n)} - \bigcup_{b\neq 0} A_b^{(n)}(a^{(p)}), & \text{若 } b=0, \end{cases}$$

则

$$B_F^{(n)}(a^{(p)}) = \{B_b^{(n)}(a^{(p)}) : b\in F_q\}$$

为$F_q^{(n)}$的一组分割，由上一章§3中定理2知，这时必有一个非线组合函数$f(x^{(n)})$，使

$$A_F[f(x^{(n)})] = B_F^{(n)}(a^{(p)}),$$

因此

$$A_b[f(x^{(n)})] \supset A_b^{(n)}(a^{(p)})$$

对任何$b\in F_q$成立。由本节引理1知，这时$f(x^{(n)})$必为$a^{(p)}$的生成函数，因此必有$C_N(a^{(p)}) \geqslant C'_N(a^{(p)})$成立，取等号成立，即(2-1-4)成立，定理得证。

定理1反映了非线性复杂度的组合特征，利用这个特征可直接利用布尔函数的性质构造a^p的生成函数，也可进一步讨论它

的递推算法。

1.3 非线性移位寄存器综合解的递推算法

该算法与 B-M 算法的思路相似，它们都是递推运算。当然，它们的运算公式与适用范围不同。我们这个递推算法适用于一般非线性复杂度的情形，对已知向量 $a^{(p)}=(a_0, a_1, \cdots, a_{p-1})$，同样记它的前部向量

$$a^{(n)}=(a_0, a_1, \cdots, a_{n-1}),\ n\leqslant p,$$

称$\langle C_n, f_n(x^{(C_n)})\rangle$为 $a^{(n)}$ 的非线性移位寄存器的综合解(以下简称非线性综合解)，若满足条件：

(i) $C_n=C_N(a^{(n)})$为 $a^{(n)}$ 的非线性复杂度。

(ii) $f_n(x^{(C_n)})$ 为 $a^{(n)}$ 的非线性生成函数(见上一章 §1 定义 3)。

与 B-M 算法相似，非线性复杂度的递推算法是由已知的综合解 $\langle C_n, f_n(x^{(C_n)})\rangle$ 与数据 $a^{(p)}$ 求 $\langle C_{n+1}, f_{n+1}(x^{(C_{n+1})}\rangle$。它的运算步骤如下：

N_1-Ⅰ 适当选择一个正整数 n_0，求出 $a^{(n_0)}$ 的非线性综合解 $\langle C_{n_0}, f_{n_0}(x^{(C_{n_0})})\rangle$。

例如，我们取 $n_0=2$，$a^{(n_0)}=(a_0, a_1)$，这时 $C_2=1$，$f_2(x)=a_1$ 就是 $a^{(2)}$ 的非线性综合解。

一般情形 n_0 还可取得大一些，这时综合解由(2-1-3)、(2-1-2)直接求得。

N_1-Ⅱ 如 $\langle C_n, f_n(x^{(C_n)})\rangle$ 为 $a^{(n)}$ 的非线性综合解，这时 $\langle C_{n+1}, f_{n+1}(x^{(C_{n+1})})\rangle$可由以下步骤确定：

(1) 如 $f(a_{n-c_n+1}, \cdots, a_n)=a_{n+1}$ 成立，则取

$$C_{n+1}=C_n,\ f_{n+1}(x^{(C_{n+1})})=f_n(x^{(C_n)}).\qquad (2\text{-}1\text{-}6)$$

(2) 如

$$f_n(a_{n-c_n+1}, a_{n-c_n+2}, \cdots, a_n)\neq a_{n+1},\qquad (2\text{-}1\text{-}7)$$

且

$$(a_{n-C_n+1}, \cdots, a_n) \notin \bigcup_{b \in F_q} A_b^{(C_n)}(a^{(n)}), \qquad (2\text{-}1\text{-}8)$$

则取 $C_{n+1}=C_n$，且

$$f_{n+1}(x^{(C_{n+1})}) = f_n(x^{(C_n)}) + [a_{n+1} - f_n(s_{n+1}^{(C_n)})] \prod_{i=1}^{C_n} \chi_{a_{n-C_n+i}}(x_i), \qquad (2\text{-}3\text{-}9)$$

其中 $\chi_a(x)$为 a 的特征函数（见(1-3-7)与(1-3-8) 定义与计算），而

$$f_n(s_{n+1}^{(C_n)}) = f(a_{n-C_n+1}, \cdots, a_n),$$

(3) 如果(2-1-7)成立，且

$$(a_{n-C_n+1}, \cdots, a_n) \in \bigcup_{b \in F_q} A_b^{(C_n)}(a^{(n)}), \qquad (2\text{-}1\text{-}10)$$

则我们定义

$$C_{n+1} = \min\{k : (a_{n-k+1}, \cdots, a_n) \notin \bigcup_{b \in F_q} A_b^{(k)}(a^{(n)})\} \qquad (2\text{-}1\text{-}11)$$

及

$$f_{n+1}(x^{(C_{n+1})}) = f_n(x_{C_{n+1}-C_{n-1}}, \cdots, x_{C_{n+1}}) + [a_{n+1} - f_n(s_{n+1}^{(C_n)})] \prod_{i=1}^{C_{n+1}} \chi_{a_{n-C_n+i}}(x_i), \qquad (2\text{-}1\text{-}12)$$

N_1-Ⅲ　重复 N_1-Ⅱ 的步骤，逐次增加向量 $a^{(n)}$ 的长，最后求得 $a^{(p)}$ 的非线性综合解 $\langle C_p, f_p(x^{(C_p)}) \rangle$。

以上算法我们称之为非线性移位寄存器综合解的递推算法，或简称为非线性综合解的递推算法。

在上述算法中，关系式(2-1-8)实际可看作(2-1-11)的特殊情形。但在计算中有时直接应用(2-1-7)更方便些。另外，在 $q=2$ 的情形，关系式(2-1-9)变为

$$f_{n+1}(x^{(C_{n+1})}) = f_n(x_{C_{n+1}-C_n+1}, \cdots, x_{C_{n+1}}) + \prod_{i=1}^{C_{n+1}} (x_i + a_{n-C_n+i} + 1). \qquad (2\text{-}1\text{-}13)$$

这时计算法更为方便.

例 对 $q=2$ 的情形,若 $p=25$,

$a^{(25)}=(00011, 01100, 11001, 11011, 00010)$, 求 $a^{(25)}$ 的非线性综合解.

解 利用 N_1-Ⅰ,Ⅱ,Ⅲ的步骤计算.

(1) 取 $n_0=9$,那么

$$a^{(9)}=(00011, 0110),$$

这时

$$A_1^{(2)}(a^{(9)})=\{(00),(01),(10),(01)\},$$
$$A_0^{(2)}(a^{(9)})=\{(00),(11)\},$$

为两个相交集合,而

$$A_1^{(3)}(a^{(9)})=\{(000),(001),(110),(101)\},$$
$$A_0^{(3)}(a^{(9)})=\{(011)\},$$

互不相交,因此 $C_9=3$,取

$$f_9(x^{(3)})=1+\bar{x}_1x_2x_3=1+x_2x_3+x_1x_2x_3,$$

显然有

$$f_9(x_1, x_2, x_3)=\begin{cases}0, x^{(3)}=(0,1,1),\\ 1, \text{其余情形},\end{cases}$$

因此

$$\langle C_9, f_9(x^{(C_9)})\rangle=\langle 3, 1+x_1x_3+x_1x_2x_3\rangle$$

为 $a^{(9)}$ 的非线性综合解.

(2) 计算

$$f_9(a_7, a_8, a_9)=f_9(110)=1\neq a_{10},$$

因为$(110)\in A_1^{(3)}(9)$,所以我们取

$$A_1^{(4)}(a^{(9)})=\{(0001),(0110),(1101)\}$$
$$A_1^{(5)}(a^{(9)})=\{(00110),(01101)\},$$

这时有

$$(a_6, \cdots, a_9)=(0110)\in A_1^{(4)}(a^{(9)}),$$

$$(a_5, \cdots, a_9) = (10110) \notin A_1^{(5)}(a^{(9)}),$$

因此取 $C_{10}=5$，而

$$f_{10}(x^{(5)}) = f_9(x_3, x_4, x_5) + x_1\bar{x}_2x_3x_4\bar{x}_5$$
$$= 1 + \bar{x}_3x_4x_5 + x_1\bar{x}_2x_3x_4\bar{x}_5.$$

(3) 计算

$$f_{10}(a_6, \cdots, a_{10}) = f_{10}(01100) = 1 = a_{11},$$
$$f_{10}(a_7, \cdots, a_{11}) = f_{10}(11001) = 1 = a_{12},$$
$$f_{10}(a_8, \cdots, a_{12}) = f_{10}(10011) = 0 = a_{13},$$
$$f_{10}(a_9, \cdots, a_{13}) = f_{10}(00110) = 1 \neq a_{14},$$

且

$$A^{(5)}(a^{(13)}) = \{(00011),(00110),(01101),$$
$$(11011),(10110),(01100),(11001),(10011)\},$$

这时

$$(a_9, \cdots, a_{13}) = (00110) \in A^{(5)}(a^{(13)}),$$

而

$$A^{(6)}(a^{(13)}) = \{(000110),(001101), \cdots\},$$

知

$$(a_8, \cdots, a_{13}) = (100110) \notin A^{(6)}(a^{(13)}),$$

因此取

$$\langle C_{11}, f_{11}(\cdot)\rangle = \langle C_{12}, f_{12}(\cdot)\rangle = \langle C_{13}, f_{13}(\cdot)\rangle$$
$$= \langle C_{10}, f_{10}(\cdot)\rangle,$$

而 $C_{14}=6$，

$$f_{14}(x^{(6)}) = f_{10}(x_2, x_3, x_4, x_5, x_6) + x_1\bar{x}_2\bar{x}_3x_4x_5\bar{x}_6$$
$$= 1 + \bar{x}_4x_5x_6 + x_2\bar{x}_3x_4x_5\bar{x}_6 + x_1\bar{x}_2\bar{x}_3x_4x_5\bar{x}_6.$$

(4) 计算

$$f_{14}(a_9, \cdots, a_{14}) = f_{14}(001100) = 1 = a_{15},$$
$$f_{14}(a_{10}, \cdots, a_{15}) = f_{15}(011001) = 1 = a_{16},$$
$$f_{14}(a_{11}, \cdots, a_{16}) = f_{15}(110011) = 0 \neq a_{17},$$

且

$$(a_{11}, \cdots, a_{16}) = (110011) \in A^{(6)}(a^{(16)}),$$
$$(a_{10}, \cdots, a_{16}) = (0110011) \in A^{(7)}(a^{(16)}),$$
$$(a_9, \cdots, a_{16}) = (00110011) \notin A^{(8)}(a^{(16)}),$$

因此

$$\langle C_{15}, f_{15}(\cdot)\rangle = \langle C_{16}, f_{16}(\cdot)\rangle = \langle C_{14}, f_{14}(\cdot)\rangle,$$

$C_{17} = 8$，而

$$f_{17}(x^{(8)}) = f_{14}(x_3, \cdots, x_8) + \bar{x}_1\bar{x}_2x_3x_4\bar{x}_5\bar{x}_6x_7x_8$$
$$= 1 + \bar{x}_6x_7x_8 + x_4\bar{x}_5x_6x_7\bar{x}_8 + x_3\bar{x}_4\bar{x}_5x_6x_7\bar{x}_8$$
$$+ \bar{x}_1\bar{x}_2x_3x_4\bar{x}_5\bar{x}_6x_7x_8.$$

(5) 计算

$$f_{17}(a_{10}, \cdots, a_{17}) = f_{17}(01100111) = 1 \neq a_{18},$$

而

$$(a_{10}, \cdots, a_{17}) = (01100111) \notin A^{(8)}(a^{(17)}),$$

因此取 $C_{18} = C_{17} = 8$，

$$f_{18}(x^{(8)}) = f_{17}(x^{(8)}) + \bar{x}_1x_2x_3\bar{x}_4\bar{x}_5x_6x_7x_8.$$

(6) 计算

$$f_{18}(a_{11}, \cdots, a_{18}) = f_{18}(11001110) = 1 = a_{19},$$
$$f_{18}(a_{12}, \cdots, a_{19}) = f_{18}(10011101) = 1 = a_{20},$$
$$f_{18}(a_{13}, \cdots, a_{20}) = f_{18}(00111011) = 0 = a_{21},$$
$$f_{18}(a_{14}, \cdots, a_{21}) = f_{18}(01110110) = 0 = a_{22},$$
$$f_{18}(a_{15}, \cdots, a_{22}) = f_{18}(11101100) = 1 \neq a_{23},$$

而 $(a_{15}, \cdots, a_{22}) = (11101100) \notin A^{(8)}(a^{(23)})$，

因此有

$$\langle C_{19}, f_{19}(\cdot)\rangle = \langle C_{20}, f_{20}(\cdot)\rangle = \cdots = \langle C_{22}, f_{22}(\cdot)\rangle$$
$$= \langle C_{18}, f_{18}(\cdot)\rangle,$$

而 $C_{23} = C_{22} = 8$，

$$f_{23}(x^{(8)}) = f_{18}(x^{(8)}) + x_1x_2x_3\bar{x}_4x_5x_6\bar{x}_7\bar{x}_8.$$

(7) 计算

$$f_{23}(a_{16}, \cdots, a_{23}) = f_{23}(11011001) = 1 = a_{24}$$

$$f_{23}(a_{17}, \cdots, a_{24}) = f_{23}(10110011) = 0 = a_{25},$$

因此得到解　$C_{25} = 8$,

$$\begin{aligned} f_{25}(x^{(8)}) = 1 &+ \bar{x}_6 x_7 x_8 + x_4 \bar{x}_5 x_6 x_7 \bar{x}_8 + x_3 \bar{x}_4 \bar{x}_5 x_6 x_7 \bar{x}_8 \\ &+ \bar{x}_1 \bar{x}_2 x_3 x_4 \bar{x}_5 \bar{x}_6 x_7 x_8 + \bar{x}_1 x_2 x_3 \bar{x}_4 \bar{x}_5 x_6 x_7 x_8 \\ &+ x_1 x_2 x_3 \bar{x}_4 x_5 x_6 \bar{x}_7 \bar{x}_8. \end{aligned} \tag{2-1-14}$$

易验证，该$\langle C_{25}, f_{25}(x^{(8)})\rangle$即为所求的 $a^{(25)}$ 的非线性综合解。

1.4　递推算法的性质

定理 2　对已知的 q 值向量 $a^{(p)}$，按递推算法 N_1-Ⅰ，N_1-Ⅱ，N_1-Ⅲ的步骤确定的$\langle C_p, f_p(x^{(C_p)})\rangle$必为 $a^{(p)}$ 的一个非线性移位寄存器综合解。

证明　首先对 n_0 的情形，由 N_1-Ⅰ的要求知，$\langle C_{n_0}, f_{n_0}(x^{(C_{n_0})})\rangle$为 $a^{(n_0)}$ 的一个非线性综合解，因此我们只要证明，若$\langle C_n, f_n(x^{(C_n)})\rangle$为 $a^{(n)}$ 的非线性综合解。这时按 N_1-Ⅱ确定的$\langle C_{n+1}, f_{n+1}(x^{(C_{n+1})})\rangle$必为 $a^{(n+1)}$ 的非线性综合解。

首先对 N_1-Ⅱ(1)的情形，有

$$f_n(a_{n-C_n+1}, \cdots, a_n) = a_{n+1} \tag{2-1-15}$$

成立，且取

$$\langle C_{n+1}, f_{n+1}(x^{(C_{n+1})})\rangle = \langle C_n, f_n(x^{(C_n)})\rangle,$$

这时 $f_n(x^{(C_n)})$为 $a^{(n)}$ 的生成函数，又由(2-1-15)知，$f_n(x^{(C_n)})$也为 $a^{(n+1)}$ 的生成函数，因此

$$C_N(a^{(n+1)}) \leqslant C_n$$

成立。另一方面，由

$$C_N(a^{(n+1)}) \geqslant C_N(a^{(n)}) = C_n$$

得 $C_n = C_N(a^{(n+1)})$，因此$\langle C_n, f_n(x^{(C_n)})\rangle$为 $a^{(n+1)}$ 的一个非线性综合解。

对于 N_1-Ⅱ(2)的情形，这时有(2-1-7)，(2-1-8)成立。同

时在(2-1-9)右边第二项总有

$$\prod_{i=1}^{C_n}\chi_{a_{n-C_n+i}}(a_{n-C_n+i-j})=\begin{cases}0, & \text{当 } j=1,2,\cdots,n-C_n+1 \text{ 时},\\ 1, & \text{当 } j=0 \text{ 时}.\end{cases}$$

因此,当 $j=1,2,\cdots,n-C_n+1$ 时,

$$f_{n+1}(a_{n-C_n-j+1},\cdots,a_{n-j})$$
$$=f_n(a_{n-C_n-j+1},\cdots,a_{n-j})=a_{n-j+1},$$

当 $j=0$ 时,

$$f_{n+1}(a_{n-C_n+1},\cdots,a_n)$$
$$=f_n(a_{n-C_n+1},\cdots,a_n)+[a_{n+1}-f_n(a_{n-C_n+1},\cdots,a_n)]$$
$$=a_{n+1},$$

所以 $f_{n+1}(x^{(C_{n+1})})$ 为 $a^{(n+1)}$ 的生成函数,这时 $C_N(a^{(n+1)})=C_n$ 的证明与 N_1-Ⅱ(1)的情形相同。

对于 N_1-Ⅱ(3)的情形,这时(2-1-7),(2-1-9)成立,且 C_{n+1}, $f_{n+1}(\cdot)$ 由(2-1-11),(2-1-12)定义。这时 $f_{n+1}(\cdot)$ 为 $a^{(n+1)}$ 的生成函数的证明与 N_1-Ⅱ(2)的情形相同,因此我们只要证

$$C_N(a^{(n+1)})=C_{n+1}$$

成立即可,这个 C_{n+1} 为(2-1-11)定义。这时首先对 $k=C_{n+1}-1$ 有

$$(a_{n-k+1},\cdots,a_n)\in\bigcup_{b\in F_q}A_b^{(k)}(a^{(n)}),$$

且必有 $k\geqslant C_n$ 成立,我们记

$$(a_{n-k+1},\cdots,a_n)\in A_b^{(k)}(a^{(n)}),$$

且有一个 $(a_{n-k+1-j},\cdots,a_{n-j})\in A_b^{(k)}(a^{(n)})$, $j\geqslant 1$, 使

$$(a_{n-k+1},\cdots,a_n)=(a_{n-k+1-j},\cdots,a_{n-j}) \qquad (2\text{-}1\text{-}16)$$

成立。

另一方面,因为 $k\geqslant C_n$,且有

$$b=f_n(a_{n-C_n+1-j},\cdots,a_{n-j}),$$
$$a_{n+1}\neq f_n(a_{n-C_n+1},\cdots,a_n),$$

因此 $a_{n+1}\neq b$,这时

$$A_0^{(k)}(a^{(n+1)}) \bigcap A_{a_{n+1}}^{(k)}(a^{(n+1)}) \neq \varnothing,$$

所以
$$C_N(a^{(n+1)}) \geqslant k = C_{n+1} - 1. \qquad (2\text{-}1\text{-}17)$$

另一方面，由 $f_{n+1}(x^{(C_{n-1})})$ 为 $a^{(n+1)}$ 的生成函数知，这时必有

$$C_N(a^{(n+1)}) \leqslant C_{n+1} \qquad (2\text{-}1\text{-}18)$$

成立，由(2-1-17)即得(2-1-18)的等号一定成立，定理得证。

定理 2 保证了以上非线性综合解的递推计算法的可靠性。这个算法的复杂度大体上可保持在 $O(p\cdot\log p)$ 数量级上，因此我们认为上述递推算法是易计算的。关于算法的复杂度问题可参看[16]中的有关论述，在此不作详细讨论。

另外，在编制 N_1-Ⅰ～N_1-Ⅲ 的运算程序中，我们还可找到一些性质来简化它们的运算过程。例如在判断

$$(a_{n-k}, \cdots, a_n) \in B^{(k)}(a^{(n)})$$

是否成立时，有性质如

$$(a_{n-k}, \cdots, a_n) \notin B_0^{(k)}(a^{(n)}),$$

则对任何 $k' \geqslant 0$，总有

$$(a_{n-k-k'}, \cdots, a_n) \notin B_1^{(k+k')}(a^{(n)}),$$

其中 $B_0^{(k)}(a^{(n)})$ 为 $A^{(k)}(a^{(n)})$ 的任何子集，而

$$B_1^{(k+k')}(a^{(n)}) = \{(a_{n-k-k'-j}, \cdots, a_{n-j}):$$
$$(a_{n-k-j}, \cdots, a_{n-j}) \in B_0^{(k)}(a^{(n)}),\ j \geqslant 1\}.$$

利用这个性质可大大简化 N_1-Ⅱ 的许多计算过程，而且可以建立相应于判断

$$(a_{n-k}, \cdots, a_n) \in A^{(k)}(a^{(n)})$$

是否成立的递推过程，对此我们不再详述了。

§2　非线性反馈移位寄存器的若干问题

2.1 关于周期序列的非线性移位寄存器的综合解

在本章 §1 中我们已给出了任意向量 $a^{(p)}$ 的非线性综合解

$\langle C_p, f_p(x^{(C_p)})\rangle$，由此即可得出任意周期序列的非线性综合解。

定义 设 $\tilde{a}=(a_0, a_1, \cdots)$ 为任一已知的周期序列，称 $\langle C, f(x^{(c)})\rangle$ 为 $\tilde{a}$ 的非线性综合解，如果

(i) $C=C_N(\tilde{a})$ 为 $\tilde{a}$ 的非线性复杂度；

(ii) $f(x^{(c)})$ 为 $\tilde{a}$ 的生成函数，具有 C 个变元。

关于周期序列 $\tilde{a}$ 的非线性复杂度与生成函数的定义在上一章§1中已给定，对此不再重复。

若我们记 $\tilde{a}$ 的一个周期为 $a^{(p)}=(a_0, a_1, \cdots, a_{p-1})$，这时利用本章§1的结果即可求出 $\tilde{a}$ 的非线性综合解。

定理1 记

$$a^{(p')}=(a_0, a_1, \cdots, a_{p'-1}),\quad p'\geqslant p$$

为 $\tilde{a}$ 的一个部分向量，相应的非线性综合解为 $\langle C_{p'}, f_{p'}(x^{(C_{p'})})\rangle$，$p'$ 满足不等式

$$p'\geqslant p+C_{p'}, \tag{2-2-1}$$

则 $\langle C_{p'}, f_{p'}(\cdot)\rangle$ 就为 $\tilde{a}$ 的非线性综合解，这时

$$\langle C, f(x^{(c)})\rangle=\langle C_{p'}, f_{p'}(x^{(C_{p'})})\rangle \tag{2-2-2}$$

成立。

利用此定理求周期序列 $\tilde{a}$ 的非线性综合解，我们只要求向量 $a^{(p+i)}$ 的非线性综合解

$$\langle C_{p+i}, f_{p+i}(x^{(C_{p+i})})\rangle,\ i=C_p, C_p+1, \cdots,$$

并且取 i_0 使

$$p+i_0\geqslant p+C_{p+i_0}(\text{或 } i_0\geqslant C_{p+i_0})$$

成立，这时取 $p'=p+i_0$ 并由(2-2-2)式得 $\tilde{a}$ 的非线性综合解，以下我们先证明该定理。

证明 分以下几点证明。

(i) 若 $\langle C_{p'}, f_{p'}(x^{(C_{p'})})\rangle$ 为 $a^{(p')}$ 的非线性综合解，且(2-2-1)成立，这时由非线性复杂度定义知

$$C_{p'}=C_N(a^{(p')})\leqslant C_N(\tilde{a})=C \qquad (2\text{-}2\text{-}3)$$

总是成立，我们只要证明 $C_{p'}\geqslant C$ 即可。记 $k=C_{p'}$，由非线性复杂度的定义知，必存在一个非线性组合函数 $f(x^{(k)})$，为向量 $a^{(p')}$ 的生成函数。这时对任何 $k\leqslant i\leqslant p'$，总有

$$a_i=f(a_{i-k},a_{i-k+1},\cdots,a_{i-1}). \qquad (2\text{-}2\text{-}4)$$

因此，对任何 $i\geqslant p'$ 或 $i>k$，我们总可找到一个 $i'=i-rp$，使 $k\leqslant i'<p'$，这时。

$$(a_{i-k},\cdots,a_{i-1},a_i)=(a_{i'-k},\cdots,a_{i'-1},a_{i'})$$

成立。因为对 i'，(2-2-4)成立，因此对 i，(2-2-4)也成立，也就是(2-2-4)对任何 i 成立。由此可见，$f(x^{(k)})$ 必为 $\tilde{a}$ 的生成函数，且

$$C_N(\tilde{a})\leqslant k=C_{p'},$$

从而得(2-2-3)的等号必成立。

(ii) 由 (i) 的证明知，(i)中的 $f_{p'}(x^{(C_{p'})})$ 为 $a^{(p')}$ 的生成函数，因为 $p'\geqslant p+C_{p'}$，所以 $f_{p'}(a^{(C_{p'})})$ 也必为 $\tilde{a}$ 的生成函数，因此(2-2-2)成立，定理得证。

例 1　在上节例题中，若 $a^{(25)}$ 为 $\tilde{a}$ 的一个周期，求 $\tilde{a}$ 的非线性综合解。

解　在上一节例题中，我们已求得 $a^{(25)}$ 的非线性综合解：$C_{25}=8$，$f_{25}(x^{(8)})$ 由(2-1-14)给定。现在我们求 $\tilde{a}$ 的非线性综合解，这时

$$\tilde{a}=(00011,01100,11001,11011,00010,$$
$$00011,01100,11001,11011,00010,\cdots)$$

为一个周期为 25 的序列，这样我们就可在例1的基础上，利用 N_1-Ⅱ的算法，求出 $\tilde{a}$ 的非线性综合解。这时有

(i) 计算

$$f_{25}(a_{18},\cdots,a_{25})=f_{25}(01100010)=1\neq a_{26}$$

且

$$(a_{18},\cdots,a_{25})=(01100010)\notin A^{(8)}(a^{(25)}),$$

因此取 $C_{26}=8$，且

$$f_{26}(x^{(8)})=f_{25}(x^{(8)})+\bar{x}_1x_2x_3\bar{x}_4\bar{x}_5\bar{x}_6x_7\bar{x}_8.$$

(ii) 计算

$$f_{26}(a_{19},\cdots,a_{26})=f_{26}(11000100)=1\fallingdotseq a_{27},$$

且

$$(a_{19},\cdots,a_{26})=(11000100)\notin A^{(8)}(a^{(26)}),$$

因此取 $C_{27}=8$，且

$$f_{27}(x^{(8)})=f_{26}(x^{(8)})+x_1x_2\bar{x}_3\bar{x}_4\bar{x}_5x_6\bar{x}_7\bar{x}_8.$$

(iii) 计算

$$f_{27}(a_{20},\cdots,a_{27})=f_{27}(10001000)=1\fallingdotseq a_{28},$$

且

$$(a_{20},\cdots,a_{27})=(10001000)\notin A^{(8)}(a^{(27)}),$$

因此取 $C_{28}=8$，且

$$f_{28}(x^{(8)})=f_{27}(x^{(8)})+x_1\bar{x}_2\bar{x}_3\bar{x}_4x_5\bar{x}_6\bar{x}_7\bar{x}_8.$$

(iv) 计算

$$f_{28}(a_{21},\cdots,a_{28})=f_{28}(00010000)=1=a_{29},$$
$$f_{28}(a_{22},\cdots,a_{29})=f_{28}(00100001)=1=a_{30},$$
$$f_{28}(a_{23},\cdots,a_{30})=f_{28}(01000011)=0=a_{31},$$
$$f_{28}(a_{24},\cdots,a_{31})=f_{28}(10000110)=1=a_{32},$$
$$f_{28}(a_{25},\cdots,a_{32})=f_{28}(00001101)=1=a_{33},$$

这对相应的非线性综合解为

$$\langle C_{29},f_{29}(\cdot)\rangle=\cdots=\langle C_{33},f_{33}(\cdot)\rangle$$
$$=\langle C_{28},f_{28}(\cdot)\rangle,$$

又由 $p'=33=p+C_{p'}=25+8$ 知，$C_{33}=8$，

$$\begin{aligned}f_{33}(x^{(8)})=1&+\bar{x}_6x_7x_8+x_4\bar{x}_5x_6x_7\bar{x}_8+x_3\bar{x}_4\bar{x}_5x_6x_7\bar{x}_8\\&+\bar{x}_1\bar{x}_2x_3x_4\bar{x}_5\bar{x}_6x_7x_8+\bar{x}_1x_2x_3\bar{x}_4\bar{x}_5x_6x_7x_8\\&+x_1x_2x_3\bar{x}_4x_5x_6\bar{x}_7\bar{x}_8+\bar{x}_1x_2x_3\bar{x}_4\bar{x}_5\bar{x}_6x_7\bar{x}_8\\&+x_1x_2\bar{x}_3\bar{x}_4\bar{x}_5x_6\bar{x}_7\bar{x}_8+x_1\bar{x}_2\bar{x}_3\bar{x}_4x_5\bar{x}_6\bar{x}_7\bar{x}_8,\end{aligned}$$

就为 $\tilde{a}$ 的非线性综合解。

2.2　非线性移位寄存器的剩余度

(1) 关于剩余度问题。在上一章 §2 中我们已给出线性移位寄存器的剩余度概念，这就是求向量 $a^{(p)}$ 的全体生成线性移位寄存器，对非线性也有类似情形。因为在上一章 §1 的讨论中知，对已给的向量 $a^{(p)}$，在它的非线性综合解 $\langle C_p, f_p(x^{(C_p)})\rangle$ 中，其非线性复杂度

$$C_p = C_N(a^{(p)})$$

是由 $a^{(p)}$ 唯一确定的，而生成函数 $f_p(\cdot)$ 可能不唯一，为了分析密码体制的安全程度，我们不仅要知道非线性复杂度的大小，还要知道生成 $a^{(p)}$ 的非线性组合函数的范围大小，这就是非线性移位寄存器的剩余度问题。确切地讲，该问题就是求 $a^{(p)}$ 的全部非线性综合解及其计数问题，一个密码体制只有当它的剩余度很大时才为安全。以下记

$$\mathscr{F}_n(a^{(p)}) = \{\text{全体 } n \text{ 元的 } a^{(p)} \text{ 的生成函数}\},\ n \geqslant C_N(a^{(p)}), \tag{2-2-5}$$

同时我们称

$$R_n(a^{(p)}) = \log\|\mathscr{F}_n(a^{(p)})\| \tag{2-2-6}$$

为 $a^{(p)}$ 的剩余度，因此剩余度的概念就是生成 $a^{(p)}$ 的非线性组合函数的范围大小。

由以上定义可知，剩余度的概念是非线性序列加密体制中的一个重要指标，对剩余度小的序列密钥体制，若数据累积到一定程度，那么利用上述非线性综合解的递推算法就可将该密钥体制打开。因此“剩余度不能使尽”是序列加密体制中的一个基本原则。

(2) 剩余度的计算公式。对已给的向量 $a^{(p)}$，由(2-1-1)我们已给出了 $A_b^{(n)}(a^{(p)})$，$b \in F_q$ 的定义，且记

$$A^{(n)}(a^{(p)}) = \bigcup_{b\in F_q} A_b^{(n)}(a^{(p)}). \tag{2-2-7}$$

这时有

定理 2 关于 $a^{(p)}$ 剩余度的计算公式为

$$R_n(a^{(p)}) = \|F_q^{(n)} - A^{(n)}(a^{(p)})\|\log q, \tag{2-2-8}$$

其中 $n\geqslant C_N(a^{(p)})$。

证明 若 $n\geqslant C_N(a^{(p)})$，则集合

$$A_b^{(n)}(a^{(p)}),\ b\in F_q$$

必互不相交，故记

$$B^{(n)}(a^{(p)}) = F_q^{(n)} - A^{(n)}(a^{(p)}),$$

且记

$$B_F^{(n)}(a^{(p)}) = \{B_b^{(n)}(a^{(p)}),\ b\in F_q\} \tag{2-2-9}$$

为 $B^{(n)}(a^{(p)})$的一个分割类。这时作

$$D_b^{(n)}(a^{(p)}) = A_b^{(n)}(a^{(p)})\bigcup B_b^{(n)}(a^{(p)}), \tag{2-2-10}$$

则

$$D_F^{(n)}(a^{(p)}) = \{D_b^{(n)}(a^{(p)}), b\in F_q\} \tag{2-2-11}$$

为 $F_q^{(n)}$ 的一个分割类，因此唯一存在一个非线性组合函数 $f(x^{(n)})$，使

$$A_F[f(x^{(n)})] = D_F^{(n)}(a^{(p)}).$$

由(2-2-10)知，$D_b^{(n)}(a^{(p)})\supset A_b^{(n)}(a^{(p)})$ 对任何 $b\in F_q$ 成立，因此 $f(x^{(n)})$是 $a^{(p)}$ 的生成函数。因为(2-2-9)的分割类有

$$q^{\|B^{(n)}(a^{(n)})\|} = q^{\|F_q^{(n)} - A^{(n)}(a^{(p)})\|}$$

多个，因此 $a^{(p)}$ 的剩余度公式(2-2-8)成立，定理得证。

由以上定理的证明即可看到，$a^{(p)}$ 的生成函数类为

$$\mathscr{F}_n(a^{(p)}) = \{f(x^{(n)}): A_F[f(x^{(n)})] = D_F^{(n)}(a^{(p)}),$$
$$D_F^{(n)}(a^{(p)})\in \tilde{D}_F^{(n)}(a^{(p)})\}, \tag{2-2-12}$$

其中 $n\geqslant C_N(a^{(p)})$，且

$$\tilde{D}_F^{(n)}(a^{(p)}) = \{\text{全体由(2-2-11)定义的 } D_F^{(n)}(a^{(p)})\}. \tag{2-2-13}$$

如我们取 $n\geqslant C_N(\tilde{a})$，同样可定义周期序列 $\tilde{a}$ 的剩余度为

$$R_n(\tilde{a}) = \log\|F_n(\tilde{a})\|, \qquad (2\text{-}2\text{-}14)$$

其中

$$F_n(\tilde{a}) = \{\text{全体 } n \text{ 元的 } \tilde{a} \text{ 的生成函数}\}. \qquad (2\text{-}2\text{-}15)$$

这时有相应的计算公式为

$$R_n(\tilde{a}) = \|F_p^{(n)} - A^{(n)}(\tilde{a})\|\log q. \qquad (2\text{-}2\text{-}16)$$

该公式的证明由本节定理即得，对此不再详述。

例 2　求本章 § 1 中例题中 $a^{(25)}$ 的剩余度。

解　因为 $C_N(a^{(25)}) = 8$，而

$$A^{(8)}(a^{(25)}) = \{(00011011),(00110110),(01101100),$$
$$(11011001),(10110011),(01100110),(11001100),$$
$$(10011001),(00110011),(01100111),(11001110),$$
$$(10011101),(00111011),(01110110),(11101100),$$
$$(11011000),(10110001),(01100010)\},$$

因此

$$R_8(a^{(25)}) = 2^8 - 18 = 238.$$

所以生成 $a^{(25)}$ 的 8 阶非线性移位寄存器有 2^{238} 个。由此可见，由 25 个数据来攻击一个 8 阶非线性移位寄存器是序列是不太可能的。同样可以指出，试图攻击一个 8 阶非线性移位寄存器的数据量应接近 $2^8 = 256$ 的大小。

我们还可以给出本节例 1 中 $\tilde{a}$ 序列的剩余度为

$$R_8(\tilde{a}) = 2^8 - \|A^{(8)}(\tilde{a})\| = 230,$$

这时生成 $\tilde{a}$ 的 8 阶非线性移位寄存器有 2^{230} 个，同样由 $\tilde{a}$ 来攻击一个 8 阶非线性移位寄存器序列也是不可能的。

§ 3　线性复杂度的组合分析

3.1　线性复杂度的组合分析问题

在上一章 § 2 中，我们已介绍了线性复杂度的作用与 B-M 算

法。该算法给出了已知向量 $a^{(n)}$ 的线性移位寄存器的综合解 $\langle l_n, f_n(x)\rangle$ 的定义及相应的一系列递推计算公式。在这一节中，我们将利用本章§1及§2的思路进一步用组合方法讨论线性复杂问题，给出一个与B-M算法不同的组合递推计算法。从形式上看，这个方法较B-M算法复杂些，但它的优点是可以同时求出向量 $a^{(p)}$ 的全部线性移位寄存器综合解。因此从这个意义上讲，本章中给出的方法在线性复杂度分析中还有其特殊的意义。

关于第一章§2及本章§1中已定义过的记号与术语，在此就不再重复了。

3.2 线性复杂度的组合表示

为了简单起见，我们先讨论 $q=2$ 的情形。设 $a^{(p)}$ 为一个二元向量，它的线性复杂度 $C_L(a^{(p)})$ 为(1-1-19)定义。现在利用本章§1的方法，先给出 $C_L(a^{(p)})$ 的组合表示。为此引进以下记号，对固定的 n，记

$$N=\{1, 2, \cdots, n\} \tag{2-3-1}$$

为部分自然数的集合，且

$$\alpha_m=\{i_1, \cdots, i_m\}\subset N, \tag{2-3-2}$$

其中

$$1\leqslant i_1<i_2<\cdots<i_m\leqslant n.$$

这时 $\alpha_m^c=N-\alpha_m$ 为 α_m 的余集，如 $\alpha_1=\{i\}$，则记

$$\alpha_i^c=N-\{i\}=N_i. \tag{2-3-3}$$

设 $x^{(n)}=(x_1, \cdots, x_n)$ 为已给的 n 维向量，则定义

$$x(\alpha_m)=(x_i, i\in\alpha_m)=(x_{i_1}, \cdots, x_{i_m}) \tag{2-3-4}$$

为 $x^{(n)}$ 的部分向量。这时有

$$x^{(n)}=(x(\alpha), x(\alpha^c))=(x_i, x(N_i))$$

成立，其中 $\alpha\subset N$。同样记全体 $x(\alpha)$ 向量空间为 $F_q(\alpha)$，这时

$$F_q(\alpha)=\prod_{i\in\alpha}F_{q,i},\quad F_{q,i}=F_q. \tag{2-3-5}$$

我们称 $F_q(\alpha)$ 为 $F_q^{(n)}$ 的部分向量空间。

在 $q=2$ 的情形，记 $d_H[x(\alpha)]$ 为 $x(\alpha)$ 的 Hamming 势，也就是 $d_H[x(\alpha)]$ 为 $x(\alpha)$ 中分量为 1 的个数。

定义

$$\begin{cases}L_0(\alpha)=\{x(\alpha):d_H[x(\alpha)]=\text{偶数}\},\\ L_1(\alpha)=\{x(\alpha):d_H[x(\alpha)]=\text{奇数}\},\end{cases} \tag{2-3-6}$$

且称之为 $F_2(\alpha)$ 中的偶奇子集。这时可定义

$$L_i^{(n)}=L_i(\alpha)\otimes F_2(\alpha^c),\ i=0.1 \tag{2-3-7}$$

为 $F_2^{(n)}$ 中的线性子集。

引理 1　关于线性子集有性质：

(i) $[L_i(\alpha)]^c=L_{i'}(\alpha)$，$i\neq i'\in\{0.1\}$。

(ii) $(L_i^{(n)})^c=[L_i(\alpha)]^c\otimes F_2(\alpha^c)$。

证明　性质(i)由 $L_i(\alpha)$ 的定义即得，因为 $x(\alpha)$ 的 Hamming 势非奇数，则一定是偶数；如 Hamming 势非偶数，则一定是奇数。此即性质(i)成立。

性质(ii)由乘积空间的性质即得，因为 $F_2(\alpha^c)$ 为 α^c 上的余空间，因此

$$\begin{aligned}(L_i^{(n)})^c&=F_2^{(n)}-L_i^{(n)}\\&=F_2(\alpha)\otimes F_2(\alpha^c)-L_i(\alpha)\otimes F_2(\alpha^c)\\&=[F_2(\alpha)-L_i(\alpha)]\otimes F_2(\alpha^c)\\&=[L_i(\alpha)]^c\otimes F_2(\alpha^c),\end{aligned}$$

性质(ii)成立，引理得证。

定理 1　$f(x^{(n)})$ 为线性函数的充要条件为 $A_0[f(x^{(n)})]$ 为线性集合 $L_0^{(n)}$ 或 $L_1^{(n)}$。

证明　如果 $f(x^{(n)})$ 为线性函数(1-1-8)，这时我们定义

$$\alpha=\{i: b_i=1,\ 1\leqslant i\leqslant n\},$$

因此

$$f(x^{(n)})=b_0+\sum_{i\in\alpha}x_i. \tag{2-3-8}$$

如果我们取 $b_0=0$,则

$$f(x^{(n)})=0 \Longleftrightarrow x(\alpha)\in L_0(\alpha),$$

这时

$$A_0[f(x^{(n)})]=L_0(\alpha)\otimes F_2(\alpha^c)=L_0^{(n)}. \tag{2-3-9}$$

如果 $b_0=1$,则

$$f(x^{(n)})=0 \Longleftrightarrow x(\alpha)\in L_1(\alpha),$$

$$A_0[f(x^{(n)})]=L_1(\alpha)\otimes F_2(\alpha^c)=L_1^{(n)}, \tag{2-3-10}$$

因此 $A_0[f(x^{(n)})]$为线性集,必要性得证.

充分性由 $f(x^{(n)})$ 关于组合表示的唯一性即得. 如 $A_0[f(x^{(n)})]$为线性集 $L_0^{(n)}$ 或 $L_1^{(n)}$,则(2-3-9)或(2-3-10)成立,因为已知线性函数(2-3-8)的组合表示为 $L_0^{(n)}$ 或 $L_1^{(n)}$,因此 $f(x^{(n)})$ 必为线性函数(2-3-8). 定理得证,

由上述证明我们可以对此定理作更精确的叙述.

定理 1′ (i) $f(x^{(n)})$为线性函数且 $b_0=0$ 的充要条件为有一个 $\alpha\subset\tilde{N}_n$ 使(2-3-9)成立.

(ii) $f(x^{(n)})$为线性函数且 $b_0=1$ 的充要条件为有一个$\alpha\subset\tilde{N}_n$ 使(2-3-10)成立.

定理 2 对于(1-1-19)定义的关于 $a^{(p)}$ 的线性复杂度的组合计算公式为

$$C_L(a^{(p)})=\min\{n:\text{存在线性集合 } L_0^{(n)},$$

$$\text{使 } A_0^{(n)}(a^{(p)})\subset L_0^{(n)} \text{ 且 } A_1^{(n)}(a^{(p)})\subset(L_0^{(n)})^c\}. \tag{2-3-11}$$

该定理的证明由本章 §1 定理 1 及本节定理 1′ 即得.

对一般 q 值的情形,我们规定 b 运算为

$$b(x)=b\cdot x,\ b^{-1}(z)=\{x: bx=z\},$$

如 $b\neq 0$，在 F_q 域中，$b^{-1}(z)=b^{-1}\cdot z$。同样可记 $z(\alpha)$，$b(\alpha)$ 为 $z^{(n)}=(z_1,\cdots,z_n)$，$b^{(n)}=(b_1,\cdots,b_n)$ 的部分向量，且定义

$$z_a(\alpha)=\{z(\alpha)\in F_q(\alpha):\sum_{i\in\alpha}z_i=a\},\ a\in F_q, \quad (2\text{-}3\text{-}12)$$

记 $b^{(n)}=(b_1,\cdots,b_n)$为一个固定向量，

$$\alpha=\alpha(b^{(n)})=\{i:b_i\neq 0\}, \quad (2\text{-}3\text{-}13)$$

这时有

$$\begin{cases} b[x(\alpha)]=(b_ix_i,\ i\in\alpha), \\ b^{-1}[z(\alpha)]=(b_i^{-1}z_i,\ i\in\alpha), \end{cases} \quad (2\text{-}3\text{-}14)$$

且

$$L_a(b^{(n)},\alpha)=\{b^{-1}[z(\alpha)]:z(\alpha)\in z_a(\alpha)\},$$

$$L_a^{(n)}(b^{(n)})=L_a(b^{(n)},\alpha)\otimes F_q(\alpha^c). \quad (2\text{-}3\text{-}15)$$

同样，我们称 $L_a^{(n)}(b^{(n)})$为 $F_q^{(n)}$ 中的线性集合，其中 $\alpha=\alpha(b^{(n)})$ 由(2-3-13)定义。

定理 3　一个 q 值 n 元函数 $f(x^{(n)})$ 为线性函数的充要条件为存在一个 $b^{(n)}$，使

$$A_a[f(x^{(n)})]=L_a^{(n)}(b^{(n)}) \quad (2\text{-}3\text{-}16)$$

对任何 $a\in F_q$ 成立

该定理的证明与本节定理 1 相似，对此不再详述，且与本节定理 2 相似，可得一般 q 值线性复杂度的组合公式

定理 4　对一般 q 值向量 $a^{(p)}$ 的线性复杂度组合公式为

$C_L(a^{(p)})=\min\{n$:存在一组线性集合 $L_a^{(n)}(b^{(n)})$，使

$$A_a^{(n)}(a^{(p)})\subset L_a^{(n)}(b^{(n)})\text{对任何 } a\in F_q\text{ 成立}\}. \quad (2\text{-}3\text{-}17)$$

证明　为证本定理，只要证明

$$L_a^{(n)}(b^{(n)}),\ a\in F_q \quad (2\text{-}3\text{-}18)$$

为 $F_q^{(n)}$ 的一组分割即可。为此，只要证明

$$L_a(b^{(n)},\alpha),a\in F_q \quad (2\text{-}3\text{-}19)$$

是 $F_q(\alpha)$的一组分割。因为 $z_a(\alpha)$，$a\in F_q$ 是 $F_q(\alpha)$的一组分割，且 $b^{-1}[z(\alpha)]$ 是

$$F_q(\alpha)\to F_q(\alpha)$$

的一个 1-1 映射。因此由(2-3-15)式知，(2-3-19)为 $F_q(\alpha)$的一组分割，所以(2-3-18)为 $F_q^{(n)}$ 的一组分割，定理得证。

3.3 线性复杂度的组合递推问题

在本节定理中，我们已给出了线性复杂度的组合公式，以下将进一步讨论它们的递推计算。为了简单起见，在本段中我们只讨论 $q=2$ 的情形。

在线性复杂度的组合公式中，问题的关键在于寻找线性集合 $L_0^{(n)}$，使

$$A_0^{(n)}(a^{(p)})\subset L_0^{(n)}, A_1^{(n)}(a^{(p)}a\subset[L_0^{(n)}]^c$$

成立，为此我们引进以下一系列记号。

设 $a^{(p)}=(a_0, a_1, \cdots, a_{p-1})$为已知的二元向量，$x^{(n)}=(x_1,\cdots, x_n)$为 F_2 上的 n 维变元向量。记

$$\alpha(x^{(n)})=\{i: i\in \hat{N}_n, x_i=1\},$$
$$\alpha(x^{(n)})^c=\hat{N}_n-\alpha(x^{(n)})$$
$$=\{i: i\in \hat{N}_n, x_i=0\}.$$

且记

$$\begin{cases}Q_0(x^{(n)})=\{\alpha'\in\hat{N}_n: \|\alpha(x^{(n)})\cap\alpha'\|=\text{偶数}\},\\ Q_1(x^{(n)})=\{\alpha'\in\hat{N}_n: \|\alpha(x^{(n)})\cap\alpha'\|=\text{奇数}\}.\end{cases}\quad(2\text{-}3\text{-}19a)$$

对任何 $0\leqslant k\leqslant p$ 与固定的 $a^{(p)}$，记

$$T_j(k)=\{t: 0\leqslant t<k \text{ 且 } a_t=j\},\ j=0,1,$$

为一列关于 $a^{(p)}$ 下标的集合。这时对任何 $t\in T_j(k)$，定义

$$Q_j(n.\ t)=Q_j[a(t-n, t-1)], j=0,1,$$

其中 $Q_j[\cdot]$为(2-3-19a)定义。这时可定义

$$\begin{cases}G_0(n, k)=[\bigcap\limits_{t\in T_1(k)}Q_1(n, t+1)]\cap[\bigcap\limits_{t\in T_0(k)}Q_0(n, t+1)],\\ G_1(n, k)=[\bigcap\limits_{t\in T_0(k)}Q_1(n, t)]\cap[\bigcap\limits_{t\in T_1(k)}Q_0(n,t)],\\ G(n, k)=G_0(n, k)\cup G_1(n, k).\end{cases}\quad(2\text{-}3\text{-}20)$$

这些集合反映了 $a^{(p)}$ 序列的结构性质.对此有

定理 5　对给定的 $a^{(p)}$,它的线性复杂度 $C_L(a^{(p)})\leqslant n$ 的充要条件为 $G_0(n,p)\neq\varnothing$,因此

$$C_L(a^{(p)})=\min\{n:G_0(n,p)\neq\varnothing\}. \tag{2-3-21}$$

在线性复杂度定义中，若 $a^{(p)}$ 的生成函数为 (1-1-13) 形式(即允许常数项 $b_0\neq0$)，$C'_L(a^{(p)})\leqslant n$ 的充要条件为 $G(n,p)\neq\varnothing$，因此

$$C'_L(a^{(p)})=\min\{n:G(n,p)\neq\varnothing\}. \tag{2-3-21a}$$

证明　若 $G_0(n,p)\neq\varnothing$,那么有一个 α' 集合,使

$$\alpha'\subset G_0(n,p)\subset\bar{N}_n.$$

这时由 $G_0(n,p)$的定义得

$$\|\alpha[a(t-n,t-1)]\cap\alpha'\|=\text{奇数} \tag{2-3-22}$$

对任何 $t\in T_1(p)$成立,且

$$\|\alpha[a(n-t,t-1)]\cap\alpha'\|=\text{偶数} \tag{2-3-23}$$

对任何 $t\in T_0(p)$成立,于是可作

$$f(x^{(n)})=\sum_{t\cdot\alpha'}x_t, \tag{2-3-24}$$

由(2-3-22)、(2-3-23)知,(2-3-24)的 $f(x^{(n)})$必为 $a^{(p)}$ 的生成函数。因为当 $t\in T_1(p)$时,$(a_{t-n},\cdots,a_{t-1})$在(2-3-24)中有奇数个项为 1,因此

$$f(a_{t-n},\cdots,a_{t-1})=1=a_t$$

成立。同理可得,当 $t\in T_0(p)$时,必有

$$f(a_{t-n},\cdots,a_{t-1})=0=a_t$$

成立,所以(2-3-24)的 $f(x^{(n)})$为 $a^{(p)}$ 的生成函数。

反之,若 $f(x^{(n)})$为 $a^{(p)}$ 的生成函数,且具(2-3-24)的形式,这时(2-3-22)、(2-3-23)必成立,因此 $G_0(n,p)\neq\varnothing$,充要条件得证。

同样可证，$G_1(n,p)\neq\varnothing$。则存在 $\alpha'\in G_1(n,p)$,使

$$f(x^{(n)}) = 1 + \sum_{i \in \alpha'} x_i \qquad (2\text{-}3\text{-}24a)$$

为 $a^{(p)}$ 的生成函数。反之，如 $a^{(p)}$ 的生成函数为 (2-3-24a)，则必有 $\alpha' \in G_1(n, p)$，因此 $G_1(n,p) \neq \varnothing$。由此定理得证。

在定理 5 的讨论中，还可得到更多的结论。如记 $\tilde{F}_{Ln}(a^{(p)})$ 为生成 $a^{(p)}$ 的全体线性反馈移位寄存器，即

$$\tilde{F}_{L,n}(a^{(n)}) = \{f(x^{(n)}): 具(2\text{-}3\text{-}24)的形式，且生成\ a^{(p)}\}。 \qquad (2\text{-}3\text{-}25)$$

这时有

定理 6 (2-3-25)的 $\tilde{F}_{L,n}(a^{(p)})$ 可表示为

$$\tilde{F}_{L,n}(a^{(p)}) = \{f(x^{(n)}) = \sum_{i \in \alpha'} x_i : \alpha' \in G_0(n, p),\ n \geqslant C_L(a^{(p)})\} \qquad (2\text{-}3\text{-}26)$$

该定理的证明由定理 5 的证明过程即得。由公式(2-3-26)可得到求生成 $a^{(p)}$ 的全部线性移位寄存器的方法，且它们可由递推算法确定。

3.4 线性复杂度的递推运算

定理 5 进一步给出了 $a^{(p)}$ 向量的组合构造，且把求 $a^{(p)}$ 的线性移位寄存器的综合解归结为求 $G_0(n, p)$ 的集合。由(2-3-20)定义可以看出，$G_0(n, p)$ 可由 $G_0(n, k)$ 递推产生。现在进一步给出它们的计算步骤。

L-Ⅰ 对已知的 $a^{(p)}$，适当的选择一对 (n_0, k_0)，直接计算 $G_0(n_0, k_0)$。一般取

$$n_0 \geqslant C_N(a^{(p)}),\ k \geqslant n_0。$$

L-Ⅱ 如 $G_0(n_i, k_i)$ 已知，则按以下步骤进行递推计算：

(1) 如 $G_0(n_i, k_i) \neq \varnothing$，$k_i = p$，且 $G_0(n_i - 1, k_i) = \varnothing$，这时有 $C_L(a^{(p)}) = n_i$，且中止递推运算，

(2) 如 $G_0(n_i, k_i) \neq \varnothing$，且 $k_i < p$，这时计算 $G_0(n_{i+1}, k_{i+1})$，其中

$$n_{i+1}=n_i,\ k_{i+1}=k_i+1.$$

(3) 如 $G_0(n_i, k_i)=\varnothing$, $k_i\leqslant p$, 则有 $C_L(a^{(p)})\geqslant n_i$, 且计算 $G_0(n_{i+1}, k_{i+1})$,其中

$$n_{i+1}=n_i+1,\ k_{i+1}=k_i.$$

L-Ⅲ　重复 L-Ⅱ 中(2), (3)运算,直到 L-Ⅱ 中(1)出现才停止运算.

在 L-Ⅱ 的运算(2),(3)中,从公式(2-3-20)知,由 $G_0(n_i, k_i)$ 求 $G_0(n_{i+1}, k_{i+1})$ 的关键在于由 $Q_j(n, t)$ 求 $Q_j(n, t+1)$ 及 $Q_j(n+1, t)$. 对此我们引进记号:

如 $\alpha=\{i_1, \cdots, i_m\}\subset\tilde{N}_n$,这时定义集合

$$\alpha\oplus 1\triangleq\{i_1+1, i_2+1, \cdots, i_m+1\}$$

及

$$\alpha\ominus 1\triangleq\begin{cases}\{i_1-1, \cdots, i_m-1\}, & \text{若 } i_1>1,\\ \{i_2-1, \cdots, i_m-1\}, & \text{若 } i_1=1.\end{cases}$$

这样,我们就可确定 $Q_j(n,t)$的递推计算公式.

L-Ⅳ　由 $Q_j(n, t)$递推计算 $Q_j(n, t+1)$有以下几种情形:

(1) 若 $a_{t-n}=a_t=0$, 这时

$$Q_j(n, t)=[Q_j(n, t-1)\ominus 1]\otimes\{\varnothing, n\},$$

其中　　$Q_j\ominus 1=\{\alpha\ominus 1;\ \alpha\in Q_j\}$, 且

$$A\otimes B=\{\alpha\cup\beta:\alpha\in A,\ \beta\in B\},$$

而$\{\varnothing, n\}$为由空集与$\{n\}$集组成的集合.

(2) 若 $a_{t-n}=1$, $a_t=0$. 这时

$$Q_j(n, t)=[Q'_{j'}(n, t-1)\ominus 1]\otimes\{\varnothing, n\}\cup[Q''_{j'}(n, t-1)\ominus 1]\otimes\{\varnothing, n\},$$

其中 $j'\neq j\in\{0, 1\}$,且

$$Q'_{j'}(n, t-1)=\{\alpha\in Q_j(n, t-1):1\notin\alpha\},$$

$$Q''_{j'}(n, t-1)=\{\alpha\in Q_j(n, t-1):1\notin\alpha\},$$

(3) 若 $a_{t-n}=0$, $a_t=1$,这时

$$Q_j(n,t)=[Q_j(n,t-1)\ominus 1]\bigcup\{[Q_{j'}(n,t-1)\ominus 1]\otimes n\},$$

其中 $j'\neq j\in\{0,1\}$,且

$$\{Q_j\ominus 1\otimes n\}=\{(\alpha\ominus 1,n):\alpha\in Q_j\}.$$

(4) 若 $a_{t-n}=a_t=1$，这时

$$Q_j(n,t)=[Q'_j(n,t-1)\ominus 1]\bigcup[Q''_{j'}(n,t-1)\ominus 1]$$
$$\cup\{[Q'_{j'}(n,t-1)\ominus 1]\otimes n\}\bigcup\{[Q''_j(n,t-1)\ominus 1]\otimes n\},$$

其中 $j'\neq j\in\{0,1\}$,且 $Q'_j(\cdot)$, $Q''_j(\cdot)$为 L-Ⅳ(2)定义。这样，就可递推计算出全体

$$Q_j(n,t),j=0,1;t=n,n+1,\cdots.$$

(5) 由$Q_j(n,t)$, $j=0,1;t=n,n+1,\cdots$，可以递推计算出$G_j(n,t)$的值,这时

$$G_j(n,t+1)=G_j(n,t)\sqcap Q_{a_t+j}(n,t+1),\quad j=0,1.$$

L-Ⅴ 由 $Q_j(n,t)$递推计算 $Q_j(n+1,t)$的情形如下：

(1) 若 $a_{t-n-1}=0$,这时

$$Q_j(n+1,t)=[Q_j(n,t)\oplus 1]\otimes\{\varnothing,1\},$$

其中 $Q_j\oplus 1=\{\alpha\oplus 1,\alpha\in Q_j\}$，且 $A\otimes B$ 的定义与 L-Ⅳ(1)中定义相同。

(2) 若 $a_{t-n-1}=1$,这时

$$Q_j(n+1,t)=[Q_j(n,t)\oplus 1]\bigcup\{[Q_{j'}(n,t)\oplus 1]\otimes 1\},$$

其中 $j'\neq j\in\{0,1\}$。

这样就可由 $Q_j(n,t)$递推计算出

$$Q_j(n+i,t),\quad i=1,2,\cdots.$$

3.5 关于线性移位寄存器的剩余度问题

线性移位寄存器的剩余度问题与非线性情形类似，即求已给向量 $a^{(p)}$ 的全体线性移位寄存器的综合解，也就是求(2-3-25)的 $\tilde{F}_{L,n}(a^{(p)})$,而且定义

$$R_{L,n}(a^{(p)})=\log\|\tilde{F}_{L,n}(a^{(p)})\|.\qquad(2\text{-}3\text{-}26a)$$

这个问题实际上已为定理 6 解决，该定理给出了 $\tilde{F}_{L,n}(a^{(p)})$的构

造，且有

$$R_{L,n}(a^{(p)}) = \log\|G_0(n,p)\|. \qquad (2\text{-}3\text{-}27)$$

利用上一章§2的讨论，我们有线性移位寄存器的剩余度公式为

定理7　对已给的 $a^{(p)}$，若

$$n = C_L(a^{(p)}) \geqslant \frac{1}{2}p, \qquad (2\text{-}3\text{-}28)$$

则 $a^{(p)}$ 的线性移位寄存器剩余度公式为

$$R_{L,n}(a^{(p)}) = (2n-p)\log q. \qquad (2\text{-}3\text{-}29)$$

如 $q=2$，则 $\log q=1$，且当 $p=2n$ 时，线性剩余度 $R_{L,n}(a^{(p)})=0$，这时综合解唯一确定。

由关系式(2-3-28)，比较(2-3-29)与(2-2-16)式知，线性移位寄存器的剩余度大大低于非线性情形。因此为保证加密体制的安全性，只有大大提高线性复杂度。

以下我们举例说明定理7及算法L-Ⅰ～L-Ⅴ的计算过程。

例　求 $a^{(18)}=(00011, 01100, 11001, 000)$ 的全体线性移位寄存器的综合解。

解　从本章§1中例1知 $C_N(a^{(15)})=6$，因此我们取 $n_0=8$。这时，

$$T_1(15)=\{3,4,6,7,10,11,14\},$$

$$T_0(15)=\{0,1,2,5,8,9,12,13\}.$$

(1) 由L-Ⅳ求出全体 $Q_j(8,t)$，$8<t\leqslant 18$。这时

$$Q_1(8,9)=\{4,5,7,8,(4,5,7),(4,5,8),(4,7,8),(5,7,8)\}$$
$$\otimes\sigma\{1,2,3,6\},$$

其中 $\sigma\{A\}$ 为 A 的全体子集系，包括空集 $\varnothing$ 与 A。同样有

$$Q_1(8,10)=\{3,4,6,7,(3,4,6),(3,4,7),(3,6,7),(4,6,7)\}$$
$$\otimes\sigma\{1,2,5,8\}$$

$$Q_1(8,11)=\{2,3,5,6,(2,3,5),(2,3,6),(2,5,6),(3,5,6)\}\otimes\sigma\{1,4,7,8\},$$

$$Q_1(8,12)=\{1,2,4,5,8,(1,2,4),(1,2,5),(1,2,8),(1,4,5),(1,4,8),(1,5,8),(2,4,5),(2,4,8),(2,5,8),(4,5,8),(1,2,4,5,8)\}\otimes\sigma\{3,6,7\},$$

$$Q_1(8,13)=\{1,3,4,7,8,(1,3,4),(1,3,7),(1,3,8),(1,4,7),(1,4,8),(1,7,8),(3,4,7),(3,4,8),(3,7,8)(4,7,8),(1,3,4,7,8)\}\otimes\sigma\{2,5,6\},$$

$$Q_1(8,14)=\{2,3,6,7,(2,3,6),(2,3,7),(2,6,7)(3,6,7)\}\otimes\sigma\{1,4,5,8\},$$

$$Q_1(8,15)=\{1,2,5,6,(1,2,5),(1,2,6),(1,5,6),(2,5,6)\}\otimes\sigma\{3,4,7,8\},$$

$$Q_1(8,16)=\{1,4,5,8,(1,4,5),(1,4,8),(1,5,8),(4,5,8)\}\otimes\sigma\{2,3,6,7\},$$

$$Q_1(8,17)=\{3,4,7,(3,4,7)\}\otimes\sigma\{1,2,5,6,8\},$$

$$Q_1(8,18)=\{2,3,6,(2,2,6)\}\otimes\sigma\{1,4,5,7,8\}.$$

同样有

$$Q_0(8,9)=\{\varnothing,(4,5),(4,7),(4,8),(5,7),(5,8),(7,8),(4,5,7,8)\}\otimes\sigma\{1,2,3,6\},$$

$$Q_0(8,10)=\{\varnothing,(3,4).(3,6),(3,7),(4,6),(4,7),(6.7),(3.4,6,7)\}\otimes\sigma\{1,2,5,8\},$$

$$Q_0(8,11)=\{\varnothing,(2,3),(2,5),(2,6),(3,5),(3,6).(5,6),(2,3,5,6)\}\otimes\sigma\{1,4,7,8\},$$

$$Q_0(8,12)=\{\varnothing,(1,2),(1,4),(1,5),(1,8),(2,4),(2,5),(2,8),(4,5),(4,8),(5,8),(1,2,4,5),(1,2,4,8),(1,2,5,8),(1,4,5,8),(2,4,5,8)\}\otimes\sigma\{3,6,7\},$$

$$Q_0(8,13)=\{\varnothing,(1,3),(1,4),(1,7),(1,8),(3,4),(3,7),(3,8),(4,7),(4,8),(7,8),(1,3,4,7),(1,3,4,8),(1,3,7,8),(1,4,7,8),(3,4,7,8)\}\otimes\{2,5,6\},$$

$$Q_0(8,14)=\{\varnothing,(2,3),(2,6),(2,7),(3,6),(3,7),(6,7),(2,3,6,7)\}\otimes\sigma\{1,4,5,8\},$$

$$Q_0(8,15)=\{\varnothing,(1,2),(1,5),(1,6),(2,5),(2,6),(5,6),(1,2,5,6)\}\otimes\sigma\{3,4,7,8\},$$

$$Q_0(8,16)=\{\varnothing,(1,4),(1,5),(1,8),(4,5),(4,8),(5,8),(1,4,5,8)\}\otimes\sigma\{2,3,6,7\},$$

$$Q_0(8,17)=\{\varnothing,(3,4),(3,7),(4,7)\}\otimes\sigma\{1,2,5,6,8\},$$

$$Q_0(8,18)=\{\varnothing,(2,3),(2,6),(3,6)\}\otimes\sigma\{1,4,5,7,8\}.$$

(2) 计算.

$$\begin{aligned}G_0(8,12)&=Q_1(8,11)\sqcap Q_1(8,12)\sqcap Q_0(8,9)\sqcap Q_0(8,10)\\&=\{1,2,(4,7),(1,5,8),(3,7,8),(6,7,8),(1,2,4,7),(1,3,4,8),(1,4,6,8),(2,3,4,5),(2,4,5,6)(4,5,7,8),(1,2,3,5,7),(1,2,5,6,7),(1,3,5,6,8),(1,2,3,4,6,7),(3,4,5,6,7,8)\},\\G_0(8,13)&=G_0(8,12)\sqcap Q_0(8,13)\\&=\{2,(4,7),(1,5,8),(6,7,8),(1,3,4,8),(2,3,4,5),(4,5,7,8),(1,2,5,6,7)(1,2,3,4,6,7),(3,4,5,6,7,8)\},\\G_0(8,14)&=G_0(8,13)\sqcap Q_0(8,14)\\&=\{(1,5,8),(6,7,8),(2,3,4,5),(1,2,3,4,6,7)\},\\G_0(8,15)&=G_0(8,14)\sqcap Q_0(8,15)=\{(6,7,8)\},\end{aligned}$$

则 $C_L(a^{(15)})=8$，且有唯一的生成多项式

$$f(x^{(8)})=x_6+x_7+x_8.$$

这时

$$G_0(8,16)=G_0(8,15)\cap Q_0(8,16)=\varnothing,$$

因此 $C_L(a^{(16)})>8$。

(3) 计算。

$$Q_j(9,k)=[Q_j(8,k)\oplus 1]\oplus\sigma\{1\}。$$

$$k=10,11,12,15,18,19,$$

$$Q_j(9,k')=[Q_j(8,k')\oplus 1]\cup\{[Q_{j'}(9,k')\oplus 1]\otimes 1\},$$

$$k'=13,14,16,17,20。$$

这时

$$\begin{aligned}G_0(9,12)&=Q_0(9,10)\cap Q_1(9,11)\cap Q_1(9,12)\\&=\{[Q_0(8,10)\cap Q_1(8,11)\cap Q_1(8,12)]\oplus 1\}\\&\quad\otimes\sigma(1),\\&=\{[2,5,(3,4),(4,6),(3,1,7),(3,7,8),(6,7,8),\\&\quad(2,4,8),(5,14),(2,3,6),(5,1,8,7),(2147),\\&\quad(2187),(5487),(356),(3148),(61487),(2345),\\&\quad(23587),(2456),(12357),(12567),(234678),\\&\quad(35614),(35618),(236147),(23618),\\&\quad(356487),(235148),(256148)]\oplus 1\}\otimes\sigma\{1\},\\G_0(9,15)&=G_0(9,12)\cap G_0(9,13)\cap G_0(9,14)\cap G_1(9,15)\\&=\{[5,(678),(123467),(234678)]\oplus 1\}\\&\quad\cup\{[(64),(4578),(12357),(12368)]\oplus\}\otimes 1,\\G_0(9,18)&=G_0(9,15)\cap G_0(9,16)\cap G_0(9,17)\cap G_1(9,18)\\&=\{(1,5,7)\}。\end{aligned}$$

由此得 $C_L(a^{(18)})=9$，且生成函数

$$f(x^{(9)})=x_1+x_5+x_7$$

为唯一解。

利用以上计算过程，我们可编制适当程序进行运算。

第 三 章

M-序列的构造与它的密钥空间

在本章中，我们在第一章 §3 至 §6 的基础上继续讨论 $M_n(q)$-序列的构造与它的密钥空间。

§1 非奇异移位寄存器的表示

1.1 非奇异移位寄存器的参数空间

在第一章 § 4 中我们已给出非奇异移位寄存器的一系列等价条件。对一般 q 值的情形，第一章 § 4 中定理 2 给出 $f(x^{(n)})$ 是非奇异的充要条件为：

(iv′) 对任何固定的 $x_2,\cdots,x_n\in F_q$，$f(x_1,x_2,\cdots,x_n)$ 为 x_1 的 1-1 函数。

或

(v′) $A_F[f(x^{(n)})]=\{A_b[f(x^{(n)})],\ b\in F_q\}$ 为 $F_q^{(n)}$ 的一个共轭类，也就是对任何 $(x_2,\cdots,x_n)\in F_q^{(n-1)}$，$A_b[f(x^{(n)})]$ 有且只有一个

$$(x_1,x_2,\cdots,x_n),\quad x_1\in F_q$$

的点。

当 $q=2$ 时，(iv′)，(v′) 条件变为

(iv) $f(x^{(n)})=x_1+f_0(x_2,\cdots,x_n)$。

(v) $A_0[f(x^{(n)})]=A_1^*[f(x^{(n)})]$，其中 A_1^* 为 A_1 的共轭集。

因此在 $q=2$ 时，全体非奇异的 $f(x^{(n)})$ 可有以下两种参数空间表示，即

S-Ⅰ $F_2^{(n-1)}$ 上的全体多项式 $f_0(x_2,\cdots,x_n)$。

如记

$$f_0(x_2,\cdots,x_n)=\sum_{i_2}^{1}\sum_{i_n=0}b_{i_1\cdots i_n}x_2^{i_2}\cdots x_n^{i_n},$$

则全体系数空间

$$\{b_{i_1\cdots i_n}:i_j\in F_2,\ j=2,\cdots,n\},$$

即为全体非奇异函数的参数空间。

S-Ⅱ 记

$$i\triangleq i(x_2,\cdots,x_n)\overset{*}{=}x_2+x_3 2+\cdots+x_n 2^{n-2},\qquad (3\text{-}1\text{-}1)$$

为 $(x_2,\cdots,x_n)$ 的一个编号集，这时 $F_2^{(n-1)}$ 可看作一个 $\{0,1,\cdots,2^{n-1}-1\}$ 集合，全体非奇异的 $f(x^{(n)})$ 可看作一个

$$\tilde{\tau}=\{\tau_i,\ i\in F_2^{(n-1)},\ \tau_i\in F_2\}\qquad (3\text{-}1\text{-}2)$$

空间，这时 $f(x^{(n)})$ 的非奇异的充要条件为有一组 (3-1-2) 的 $\tilde{\tau}$，使

$$A_0[f(x^{(n)})]=\{(\tau_i,i):i\in F_2^{(n-1)}\},$$
$$A_1[f(x^{(n)})]=\{(\tilde{\tau}_i,i):i\in F_2^{(n-1)}\}。\qquad (3\text{-}1\text{-}3)$$

这时我们称全体(3-1-2)的 $\tilde{\tau}$ 为非奇异移位寄存器的参数空间。

对一般 q 值的情形，我们可以推广 S-Ⅰ 与 S-Ⅱ 的形式，有

S-Ⅲ 记 $f(x^{(n)})$为(1-4-3)的分解式，即

$$f(x^{(n)})=\sum_{k\in Fq}x_1^k f_k(x_2,\cdots,x_n),\qquad (3\text{-}1\text{-}4)$$

这时非奇异的充要条件为

$$f_0(x_2,\cdots,x_n),\cdots,f_{q-1}(x_2,\cdots,x_n))\in B_q,\qquad (3\text{-}1\text{-}5)$$

其中 B_q 空间为(1-4-2)定义。

S-Ⅳ 在(3-1-1)的编号下，记

$$\tilde{\tau}=\{\tau_i: i\in F_q^{(n-1)}\} \tag{3-1-6}$$

为一族 $F_q\to F_q$ 的置换（这时每个 τ_i 为 F_q 上的置换），这时 $f(x^{(n)})$ 为非奇异的充要条件为

$$A_0[f(x^{(n)})]=\{(\tau_i^{-1}(b), i): i\in F_q^{(n-1)}\}, \tag{3-1-7}$$

对任何 $b\in F_q$ 成立。我们有时称 (3-1-6) 的 $\tilde{\tau}$ 为 $n-1$ 阶置换族，并记之为 $\tilde{\tau}^{(n-1)}$。

这时，我们可把(3-1-6)的全体 $\tilde{\tau}$ 看作全体非奇异 $f(x^{(n)})$ 的参数空间。现在进一步讨论 S-Ⅲ 与 S-Ⅳ 表示之间的关系。

1.2 非奇异移位寄存器参数空间的关系定理

在 S-Ⅲ，S-Ⅳ 中，我们已给出非奇异 $f(x^{(n)})$ 的两种充要条件，它们分别由向量函数

$$(f_0(x^{(n-1)}), \cdots, f_{q-1}(x^{(n-1)}))=f^{(q)}(x_i^{(n-1)}) \tag{3-1-8}$$

与(3-1-6)的置换族 $\tilde{\tau}$ 表示。现在讨论它们的关系。

首先对 $q=2$ 的情形，我们只要讨论函数 $f_0(x_2, \cdots, x_n)$ 与(3-1-2)的函数 τ_i 之间关系即可。如 $f(x^{(n)})=x_1+f_0(x_2, \cdots, x_n)$ 成立，则

$$\begin{aligned}A_0[f(x^{(n)})]&=(x_1=0)\otimes A_0[f_0(x_2, \cdots, x_n)]\\&\bigcup(x_1=1)\otimes A_1[(f_0(x_1, \cdots, x_n)]\end{aligned} \tag{3-1-9}$$

成立。对于(3-1-2)的 $\tilde{\tau}$，我们定义，

$$B_j(\tilde{\tau})=\{i: i\in F_2^{(n-1)}, \tau_i=j\}, \tag{3-1-10}$$

这时有

$$\begin{aligned}A_0[f(x^{(n)})]&=\{(\tau_i, i), i\in F_2^{(n-1)}\}\\&=B_0'(\tilde{\tau})\bigcup B_1'(\tilde{\tau}),\end{aligned} \tag{3-1-11}$$

其中

$$B_j'(\tilde{\tau})=\{(j, i): i\in B_j(\tilde{\tau})\}.$$

这样我们有

定理 1 如 $f(x^{(n)})$ 为非奇异的，这时 $f(x^{(n)})$ 必同时具有

S-Ⅰ与S-Ⅱ的两种表示形式，且

$$A_0[f_0(x_2, \cdots, x_n)] = B_0(\tilde{\tau}), \tag{3-1-12}$$

其中 $B_j(\tilde{\tau})$ 由(3-1-10)定义。

证明 因为 $f(x^{(n)})$是非奇异的，因此 $f(x^{(n)})$同时具有S-Ⅰ，S-Ⅱ的两种表示形式，所以有(3-1-9)与(3-1-11)成立，这时 $A_0[f(x^{(n)})]$ 在 $x_1=0$ 处切口分别为 $A_0[f_0(x_2, \cdots, x_n)]$ 与 $B_0(\tilde{\tau})$，因此必有(3-1-12)成立。定理得证。

由此定理知，对 $q=2$ 的情形，非奇异函数的S-Ⅰ，S-Ⅱ两种表示形式由(3-1-12)即可相互确定。

对于一般 q 值的情形，非奇异函数 $f(x^{(n)})$ 的S-Ⅲ，S-Ⅳ的表示形式实际上是一致的，因为对任何置换族 $\tilde{\tau}$ 的每个置换 $\tau_i(\cdot)$ 可表示成多项式

$$\tau_i(x) = b_{i0} + b_{i1}x + \cdots + b_{iq-1}x^{q-1}, \tag{3-1-13}$$

这时

$$b_i^{(q)} = (b_{i0}, \cdots, b_{iq-1}) \in B_q$$

与S-Ⅲ的表示形式

$$f^{(q)}(x^{(n-1)}) = (f_0(x^{(n-1)}), \cdots, f_{q-1}(x^{(n-1)})) \in B_q$$

是一致的，其中 $x^{(n-1)} = (x_2, \cdots, x_n)$，当

$$i = i(x_2, \cdots, x_n)$$

时，必有

$$f_j(x^{(n-1)}) = b_{ij},\ j \in F_q \tag{3-1-14}$$

成立，这样就可由置换族 $\tilde{\tau}$ 完全确定非奇异的 $f(x^{(n)})$（或 $f^{(q)}(x^{(n-1)})$），反之亦然。它们的确定过程可按第一章 §3 非线性组合函数的组合表示写出，对此就不再详述。

1.3 非奇异函数的递推性

由S-Ⅲ或S-Ⅳ我们给定了 $F_q^{(n)}$ 上的全体非奇异函数，这样，就可由S-Ⅲ或S-Ⅳ直接写出任意 n 阶非奇异函数 $f(x^{(n)})$。为了简化 $f(x^{(n)})$ 的构造过程，我们进一步讨论非奇异函数的递

推性质。

定理 2 若 $f_b(x^{(n)})$，$b\in F_q$ 为 q 个 n阶 非奇异函数，则

$$f(x^{(n+1)})=\sum_{b\in F_q}\chi_b(x_{n+1})f_b(x^{(n)}) \qquad (3\text{-}1\text{-}15)$$

必为 $n+1$ 阶非奇异函数。反之，若 $f(x^{(n+1)})$ 为非奇异的，则

$$f_b(x^{(n)})=f(x_1,\cdots,x_n,b),\ b\in F_q \qquad (3\text{-}1\text{-}16)$$

为非奇异的，且(3-1-15)成立。

证明 若 $f(x^{(n+1)})$由(3-1-15)构成，$f_b(x^{(n)})$为非奇异的，这时对任何固定的 $a^{(n)}=(a_2,\cdots,a_{n+1})$，必有

$$f(x_1,a_2,\cdots,a_{n+1})=f_{a_{n+1}}(x_1,a_2,\cdots,a_{n+1}) \qquad (3\text{-}1\text{-}17)$$

成立。因为 $f_{a_{n+1}}(x^n)$ 是非奇异的，所以 (3-1-17)的函数是 x_1 的 1-1 对应函数，此即 $f(x^{(n+1)})$ 的非奇异性成立。

反之，由 $f(x^{(n+1)})$ 的非奇异性及(3-1-16)式知 $f_b(x^{(n)})$必为非奇异的，定理得证。

在非奇异函数的组合表示中，若记

$$\tilde{\tau}_b^{(n)}=\{\tau_{bi}(\cdot),\ i\in F_q^{(n)}\},\ b\in F_q \qquad (3\text{-}1\text{-}18)$$

为一组 n 阶置换族，又记

$$\tilde{\tau}^{(n+1)}=\{\tau_{bi}(\cdot),\ i\in F_q^{(n)},\ b\in F_q\}, \qquad (3\text{-}1\text{-}19)$$

则 $\tilde{\tau}^{(n+1)}$ 为一 $n+1$ 阶置换族。如记

$$j(b,i)\overset{*}{=}i+bq^n, \qquad (3\text{-}1\text{-}20)$$

则 $\tilde{\tau}^{(n+1)}$ 又可表示为 $\{\tau_j(\cdot),\ j\in F_q^{(n+1)}\}$，这时由 (3-1-7) 与 $\tilde{\tau}_b^{(n)}$，$b\in F_q$，$\tilde{\tau}^{(n+1)}$ 分别可以确定非奇异函数

$$f_b(x^{(n)}),\ b\in F_q \text{ 及 } f(x^{(n+1)}),$$

且 (3-1-15) 式成立，因此我们称 (3-1-19) 的 $\tilde{\tau}^{(n+1)}$ 为 $\{\tilde{\tau}_b^{(n)},\ b\in F_q\}$ 的合成，而 $\{\tau_b^{(n)},\ b\in F_q\}$ 为(3-1-19) 的 $\tilde{\tau}^{(n+1)}$ 的分解。这样我们有

定理 3 如果 $f(x^{(n+1)})$ 为非奇异函数，且有分解式(3-1-15)成立，则 $f(x^{(n+1)})$ 与 $f_b(x^{(n)})$ 相应的组合表示 $\tilde{\tau}^{(n+1)}$ 与 $\tilde{\tau}_b^{(n)}$ 有

(3-1-18)与(3-1-19)的分解形式。

反之，若 $\tau^{(n+1)}$ 与 $\tau_b^{(n)}$ 有(3-1-18)与(3-1-19)的分解，则相应的 $f(x^{(n+1)})$ 与 $f_b(x^{(n)})$ 为非奇异的，且有(3-1-15)的关系成立。

在定理2和3中，我们的合成与分解均对 x_{n+1} 变量而言。实际上，这两个定理均可推广到任何 $x_2, \cdots, x_{n+1}$ 变量，这时(3-1-15)，(3-1-16)可推广为

$$f(x^{(n+1)}) = \sum_{b \in F_q} \chi_b(x_k) f_{kb}(x^{(n+1)}), \qquad (3\text{-}1\text{-}15)$$

其中 $2 \leqslant k \leqslant n+1$，且

$$f_b(x^{(n+1)}) = f_b(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{n+1}).$$

而(3-1-20)可推广为

$$j(b, i) \stackrel{*}{=} i(\mathrm{mod} q^k + bq^{k-1} + [i - i(\mathrm{mod} q^k)]q. \qquad (3\text{-}1\text{-}20a)$$

利用以上方法，我们即可构造和计算全体 n 阶非奇异函数。

例 对于 $q=2, n=6$ 的情形，如果

$$\tau^{(5)} = \{\tau_i : i = 0, 1, \cdots, 31\}$$
$$= \{11011, 00001, 00101, 11110, 11000, 10101, 10\},$$

求相应的非奇异函数。

解 由(3-1-10)知

$$B_0(\tau) = \{2, 5, 6, 7, 8, 9, 11, 12, 14, 20, 23, 24, 25, 27, 29, 31\}$$
$$= \{(01000), (10100), (01100), (11100), (00010), (10010), (11010), (00110), (01110), (00101), (11101), (00011), (10011), (11011), (10111), (11111)\}.$$

这时

$$f_6(x_2, \cdots, x_6) = \bar{x}_6\{\bar{x}_5[\bar{x}_4 x_3 x_2 + x_4(x_2 + x_3 + x_2 x_3)]$$

$$+x_5[\bar{x}_4(\bar{x}_3+x_3x_2)+x_4\bar{x}_2]\}$$
$$+x_6\{\bar{x}_5x_4(\bar{x}_2+x_3)+x_5[\bar{x}_4(\bar{x}_3+x_3x_3)+x_4x_3]\}$$
$$=x_3+x_5+x_2x_3+x_2x_4+x_3x_4+x_4x_6+x_3x_4x_5$$
$$+x_3x_4x_6+x_3x_5x_6+x_2x_3x_4x_5+x_2x_3x_5x_6$$
$$+x_2x_4x_5x_6$$

即为所求。

对一般 q 值函数情况更为复杂些，对此不再详述。

1.4 非奇异复杂度问题

对于任何一个 q 值向量 $a^{(p)}=(a_0, a_1, \cdots, a_{p-1})$（或周期序列 $\tilde{a}=(a_0, a_1, \cdots)$），我们称

$$C_s(a^{(p)})=\min\{n:\text{存在一个非奇异函数 } f(x^{(p)}) \text{生成向量 } a^{(p)}\} \quad (3\text{-}1\text{-}21)$$

为 $a^{(p)}$ 的非奇异复杂度，这时关于非线性复杂度的许多性质可以推移到非奇异复杂性情形。以下讨论向量 $a^{(p)}$ 均为非周期的，即对任何 $0<p'<p$，$i=1, 2, \cdots, p-p'$，

$$(a_i, \cdots, a_{i+p'-1}) \neq (a_0, \cdots, a_{p'-1}).$$

定理 4 如果 $a^{(p)}$ 是非周期向量，则

$$C_s(a^{(p)})=\min\{n:\text{全体 } (a_{t-n}, \cdots, a_{t-1}),\ t=n, n+1, \cdots, p-1 \text{ 互不相同}\}, \quad (3\text{-}1\text{-}22)$$

证明 该定理证明与(2-1-2)相似，若有非奇异的 $f(x^{(n)})$ 生成 $a^{(p)}$，则

$(a_{t-n}, a_{t-n+1}, \cdots, a_{t-1})$，$t=n, m+1, \cdots, p-1$，必互不相同，否则若有一对，$(t, t')$，$n\leqslant t\neq t'\leqslant p-1$，使

$$(a_{t-n}, \cdots, a_{t-1})=(a_{t'-n}, \cdots, a_{t'-1})$$

成立，这时由非奇异函数的性质及 $f(x^{(n)})$ 生成 $a^{(p)}$ 的条件，必有

$$a_{t-n-i}=Q_{t'-n-i},\ i=0, 1, \cdots.$$

成立。不失一般性，如我们讨论 $t'>s$，$pt=t'-t$，则必有 $0\leqslant p'\leqslant$

$p-1$，

$$(a_0, \cdots, a_{n-1}) = (a_{pt}, \cdots, a_{pt+n-1})$$

成立，且对任何 $j=1, 2, \cdots$，均有 $a_{n-1+j} = a_{pt+n-1+j}$ 成立，这与 $a^{(p)}$ 的非周期性质矛盾。

反之，若 $(a_{t-n}, \cdots, a_{t-1})$，$t=n, \cdots, p-1$ 互不相同，我们记

$$\tau_t = (a_{t-n+1}, \cdots, a_{t-1}) \in F_q^{(n-1)},$$

而记 $\tau_z(a)$ 为 $F_q \to F_q$ 的 1-1 映射，使当 $z=z_t$ 时，

$$\tau_z(a_{t-n}) = a_t \tag{3-1-23}$$

成立，这样的 $\tau_z(a)$ 必存在。因为每个 $z \in F_q^{(n-1)}$，使

$$(a, z) = (a_{t-n}, z_t)$$

成立的 t 最多只有一个，这样由 $(\tau_z(a), z)$ 就可构造非奇异函数 $f(x^n)$ 且生成 $a^{(q)}$。定理得证。

从第二章的讨论，同样可建立非奇异函数的综合解及相应的递推公式，这时，我们始终取非奇异综合解 $\langle C_n, f_n(x^{(k)})\rangle$ 中的 $f_n(x^{(k)})$ 为非奇异函数，相应的组合表示为

$$\tau_z^{(k)}(a),\ z \in F_q^{(k-1)},$$

除了 $f(x^{(k+1)})$ 满足 $f(x^{(k)})$ 在 $a^{(n)}$ 上的扩张条件。若 $f(x^{(k+1)})$ 的组合表示记为

$$(\tau_{z'}^{(k+1)}(a),\ z') : z' \in F_q^{(k)},$$

$\tau_{z'}^{(k+1)}(a)$ 满足条件：当 $z' = (a_{t+1}, \cdots, a_{t+k})$ 时，

$$\tau_{z'}^{(k+1)}(a_t) = a_{t+k+1} = \tau_z^{(k)}(a_{t+1}),$$

对任何 $0 \leqslant t \leqslant n-k-1$ 成立，其中 $z = (a_{t+2}, \cdots, a_{t+k}) \in F_q^{(k-1)}$。

同样可作 $f(x^{(k+2)})$ 为 $f(x^{(k+1)})$ 在 $a^{(n)}$ 上的扩张，这时 $f(x^{(k+2)})$ 为 $f(x^{(k)})$ 的二次扩张（非奇异扩张）。

在 N_1-Ⅱ 的递推运算中，如 (2-1-7)，(2-1-9) 同时成立，由 (2-1-9)，(2-1-10) 知 $C_{n+1} > C_n$，记 $k = C_{n+1}$，$k' = C_n$，这时作 $f_{n+1}(x^{(k)})$ 为 $f_n(x^{(k)})$ 的 $k'-k$ 次非奇异扩张，因为

$$z=(a_{n-k+1},\cdots,a_n)\notin\bigcup_{b\in F_q}A_b^{(k)}(a^{(\tau)}),$$

所以我们可以取 $\tau_z(a)$ 为任一置换函数，且满足条件

$$\tau_z(a_{n-k})=a_{n+1},$$

这时 $f_{n+1}(x^{(k)})$ 必为 $a^{(n+1)}$ 的非奇异生成函数，从而可得到一系列相应的递推运算，求出 $a^{(p)}$ 的非奇异综合解。

关于非奇异函数的剩余度问题，可同样按非线性剩余度的讨论进行定义。若记 $\mathscr{F}_{1,n}(a^{(p)})$ 为 $a^{(p)}$ 的全体非奇异生成函数 $f(x^{(\tau)})$，这时称

$$R_{1,n}(a^{(p)})\triangleq\log\|\mathscr{F}_{1,n}(a^{(p)})\| \tag{3-1-24}$$

为 $a^{(p)}$ 的非奇异剩余度。对任何

$$z=(a_1,\cdots,a_{n-1})\in F_q^{(n-1)}.$$

记 $k(z)$ 为 z 在 $a^{(p)}$ 中出现的次数，而 $N(k)$ 为 $k(z)=k$ 的 z 的个数，则有

定理 5 $a^{(p)}$ 的非奇异剩余度为

$$R_{1,n}\triangleq\sum_{k=0}^{q}N(k)\log[(q-k)!], \tag{3-1-25}$$

当 $q=2$ 时，就有 $R_{1,n}=N(0)$ 成立。

证明 因为在非奇异函数的选取中，对每个 $z\in F_q^{(n-1)}$，$\tau_z(a)$ 函数有 $k(z)$ 个值为 $a^{(p)}$ 决定，另外 $q-k(z)$ 个点的值为任何使 $\tau_z(a)$ 为置换函数，因此它们取法有 $[q-k(z)]!$ 种，故

$$\|\mathscr{F}_{1,n}(a^{(p)})\|\triangleq\prod_{z\in F_q^{(n-1)}}\{[q-k(z)]!\}$$

$$\triangleq\prod_{k=0}^{q}[(q-k)!]^{N(k)}$$

成立，此即(3-1-25)成立。

定理 6 若记 $C_N(a^{(p)})$，$C_S(a^{(p)})$ 分别为 $a^{(p)}$ 的非线性复杂度与非奇异复杂度，这时必有

$$C_N(a^{(p)})\leqslant C_S(a^{(p)})\leqslant C_N(a^{(p)})+1 \tag{3-1-26}$$

成立。

证明 (3-1-26)的第一个不等式是显然的，对第二个不等式，如 $n=C_N(a^{(p)})$，则

$$(a_t, a_{t+1}, \cdots, a_{t+n}),\ 0\leqslant t<p-n-1,$$

必互不相同，否则与 $a^{(p)}$ 的非周期性矛盾。因此 (3-1-26) 必成立。定理得证。

关系式(3-1-26)在第四章中还会用到。

§2 M-序列的组合构造与它的密钥空间

如前所述，在本章中我们的主要目的是进一步研究 M-序列的构造及它们的参数空间表示。为此，我们采用联系矩阵，剪接算子(或剪接递推算子)，组合表示性质等方法进行分析。在本节中，我们讨论用联系矩阵表示一般的 q 值 n 阶 M-序列(以下记为 $M_n(q)$-序列)。为了简单起见，我们称产生 $M_n(q)$-序列的移位寄存器为 $M_n(q)$-移位寄存器，相应的图与多项式为 $M_n(q)$-图与 $M_n(q)$-多项式。如 $f(x^{(n)})$ 为 $M_n(q)$-多项式，则对任何初始状态 $(a_0, a_1, \cdots, a_{n-1})$，由 $f(x^{(n)})$ 产生的序列 $\tilde{a}=(a_0, a_1, a_2, \cdots)$总是 $M_n(q)$-序列，这时 $M_n(q)$-图为 $G_n(q)$中的极大圈。

2.1 完备回路的编号表示

在第一章§5和§6中我们已经指出，全体$G_{n+1}(q)$图中的极大圈(即 $M_{n+1}(q)$-图)与全体 $G_n(q)$ 中的完备回路相互唯一确定。如 (1-6-9) 所表示，记 $\vec{W}(S_0, n, q)$ 为 $G_n(q)$ 中的全体完备回路，且以 $S_0\in F_q^{(n+1)}$ 为起弧。这时对任何 $W\in\vec{W}(S_0, n, q)$，确定一个编号集

$$I(W, S_0)=\{I(s, W, S_0): s\in F_q^{(n)}\}, \qquad (3\text{-}2\text{-}1)$$

其中 $I(s, W, S_0)$ 由 (1-6-3) 定义，且

$$L(W, S_0)=\{(s, a_n(s, i)): s\in F_{q,0}^{(n)}\} \qquad (3\text{-}2\text{-}2)$$

为 $G_n(q)$ 中极大反树的全体弧，$F_{q,0}^{(n)}$ 为 (1-6-6) 定义。

反之，若

$$I(S_0)=\{I(s, S_0): s\in F_q^{(n)}\} \tag{3-2-3}$$

为一组编号集，其中

$$I(s, S_0)=\{(s, a_n(s, i)), i=1, \cdots, q\} \tag{3-2-4}$$

为 $G_n(q)$ 图中 x 点出弧的一个编号次序，$S_0=(s_0, a_n^0)$，则在(3-2-4)中

$$(s_0, a_n(s_0, 1))=(s_0, a_n^0)。$$

记

$$L(S_0)=\{(s_0, a_n(s_0, q)):\ s\in F_{q,0}^{(n)}\}, \tag{3-2-5}$$

其中 $F_{q,0}^{(n)}=F_q^{(n)}-\{s_0\}$。由第一章§6定理2知，若 $G(S_0)=\{F_q^{(n)}, L(S_0)\}$ 为反树图，则必有 $G_n(q)$ 中的一完备回路 W，使

$$I(W, S_0)=I(S_0), \tag{3-2-6}$$

或对任何 $s\in F_q^{(n)}$，

$$I(s, W, S_0)=I(s, S_0) \tag{3-2-7}$$

成立。如果记 $\tilde{L}_T(S_0)$ 为全体(3-2-5)的 $L(S_0)$，使 $G(S_0)$ 为反树，这时我们称

$$\tilde{L}_0(S_0)=\{L(S_0): L(S_0)\in\tilde{L}_T(S_0)\} \tag{3-2-8}$$

为全体 $G_n(q)$ 中完备回路的参数空间，或 $G_{n+1}(q)$ 中全体 $M_{n+1}(q)$-序列的参数密钥空间，显然

$$\tilde{L}_0(S_0),\ \tilde{W}(S_0, n, q),\ \tilde{M}(S_0, n+1, q) \tag{3-2-9}$$

为三个相互 1-1 对应的空间，所以我们有时简称 $\tilde{L}_0(S_0)$ 为全体 $M_n(q)$-移位寄存器的密钥空间。由 $\tilde{L}_0(S_0)$ 的定义(3-2-8)知，构造 $\tilde{L}_0(S_0)$ 的关键在于 $\tilde{L}_T(S_0)$ 的构造。

2.2 $\tilde{L}_T(S_0)$ 的联系矩阵构造

为构造 $\tilde{L}_T(S_0)$，我们先采用联系矩阵的表示方法。设 $B[G_n(q)]$ 为 $G_n(q)$ 的联系矩阵，相应的元

$$d_{ij}=\begin{cases}1, & \text{若 } (j, i)\in L_n(q),\\ 0, & \text{否则。}\end{cases} \tag{3-2-10}$$

其中 i，j 为 $F_q^{(n)}$ 中向量的编号，即对任何 $s=(a_0, a_1, \cdots, a_{n-1}) \in F_q^{(n)}$，记

$$i=i(s) \triangleq a_0+a_1q+\cdots+a_{n-1}q^{n-1}, \qquad (3\text{-}2\text{-}11)$$

而弧 (j, i) 即 (s_j, s_i)，s_j，s_i 为 (3-2-11) 的逆。

定义 1 两个同阶的联系矩阵 $B=(d_{ij})$，$B'=(d'_{ij})$，称 B' 为 B 的子矩阵，如 $d'_{ij} \leqslant d_{ij}$。此即由 $d_{ij}=0$ 必有 $d'_{ij}=0$。

引理 1 由联系矩阵定义，有

(1) 若 $G=\{A, L\}$，$G'=\{A', L'\}$，且 $A=A'$，则 G' 为 G 的子图的充要条件为 $B(G')$ 为 $B(G)$ 的子矩阵。

(2) 若 $G=\{A, L\}$. $A=F_q^{(n)}$，则 G 为 n 阶移位寄存器图的充要条件为：

(i) $B(G)$ 为 $B[G_n(q)]$ 的子矩阵；

(ii) 对任何 $j=0, 1, \cdots, q^n-1$，

$$\sum_{i=0}^{k_n} d_{ij}=1 \qquad (3\text{-}2\text{-}12)$$

成立，其中 $k_n=q^n-1$。

(3) $T=\{A_n, L\}$ 为 $G_n(q)$ 的极大反树图且以 s_0 为根的充要条件为：

(i) $B(T)$ 为 $B([G_n(q)]$ 的子矩阵；

(ii) (3-2-12) 对任何 $i=1, 2, \cdots, k_n$ 成立。

(iii) $\Delta_1(T)=1$，其中 $\Delta_1(T)$ 为 (1-5-10) 定义。

该引理由第一章讨论的性质直接推出，在此不再详述。由此可得，为构造 $\tilde{L}_T(X_0)$，我们只要构造全体具该引理 1 中(3)的条件(i)，(ii)，(iii) 的联系矩阵即可。以下记

$$\tilde{B}_T(n, q)=\{\text{全体 } (k_n+1)\times(k_n+1)\text{阶的二元矩阵，满足引理 1 中(3)的条件(i)}\sim\text{(iii)}\}. \qquad (3\text{-}2\text{-}13)$$

这时 $\tilde{L}_T(S_0)$ 与 (3-2-13) 的 $\tilde{B}_T(n, q)$ 矩阵类 1-1 对应，因此以下进一步讨论 $\tilde{B}_T(n, q)$ 的表示即可。同样记

$$\alpha(k)=\{j_1,\cdots,j_k\}\subset\{1,2,\cdots,n\},$$

其中 $1\leqslant j_1<j_2<\cdots<j_k\leqslant n$。

定义 2 (i) 我们称一个 $n\times n$ 阶矩阵 $B=(d_{ij})$ 是 (n,α_k)型的，如 $d_{ij}=0$ 或 1，且满足条件：$d_{ii}=0$，$i=1,\cdots,n$，且

$$\sum_{i=1}^{n}d_{ij}=\begin{cases}0, & \text{若 } j\in\alpha_k,\\ 1, & \text{若 } j\notin\alpha_k.\end{cases}\tag{3-2-14}$$

(ii) 称一个 $n\times n$阶矩阵 $B=(d_{ij})$ 为 T 型的，如存在一组 $\{\alpha_1,\cdots,\alpha_r\}$ 为 $N=\{1,\cdots,n\}$ 的分割，使 B 为一个 (n,α_1) 型矩阵，且 $B_{\alpha_1\cdots\alpha_i}$ 为 (n_i,α_{i+1}) 型矩阵，$i=1,2,\cdots,r-1$，其中

$$n_i=n-\|\alpha_1\|-\|\alpha_2\|-\cdots-\|\alpha_i\|,$$

且 B_α 为 B 矩阵划去 $\alpha=\{j_1,\cdots,j_k\}$ 中全体 j_i 所在的行、列后所得的矩阵。

(iii) 如 B 是 $B[G_n(q)]$ 的子矩阵，且为 (q^n,α)型的，我们称 B 为 (n,q,α)型矩阵。同样可定义，若 B 是 $B[G_n(q)]$ 的子矩阵，且是 T 矩阵，我们称 B 为 $T_n(q)$型矩阵。

以下记 E_n 为 $n\times n$ 阶幺矩阵，若 B 为 $n\times n$ 阶矩阵，则定义

$$Q(B)=E_n-B,\quad \Delta(B)=\|Q(B)\|。\tag{3-2-15}$$

这时有以下性质：

引理 2 (i) 全体 $(n,\alpha(k))$ 的矩阵的个数为 n^{n-k} 个，而全体 $(n,q,\alpha(k))$ 矩阵的个数为 q^{qn-k} 种。

(ii) 若 B 是一个(n,α)型的矩阵，则

$$\Delta(B)=\Delta_\alpha(B)=\|Q_\alpha(B)\|,\tag{3-2-16}$$

其中 $\Delta_\alpha(B)$ 为 $\Delta(B)$ 划去 α 中所在行、列后的行列式的值。因此 $\Delta(B)\neq 0$ 的充要条件为 B 是 T 型矩阵，这时必有 $\Delta(B)=1$。

证明 对于(i)的性质是显然的，因为在 $(n,\alpha(k))$ 矩阵中，有 k 个列固定为零向量，其余 $n-k$ 个列只有一个分量为 1，其余分量为零，因此有 n 种取法，且 $(n,\alpha(k))$ 矩阵的取法有 n^{n-k}

种。而在$(n,\alpha(k))$矩阵中，有k列为零向量，其余q^n-k列有一个分量为1，其余为零。因为B是$B[G_n(q)]$的子矩阵，所以这q^n-k个列中，每个列的取法只有q种，因此$(n,q,\alpha(k))$矩阵的个数为q^{q^n-k}种。

关于性质(ii)的证明也是十分明显的。若B是(n,α)型，那么在$Q(B)=E-B=(d'_{ij})$中，若$j\in\alpha$，则必有

$$d'_{ij}=\begin{cases}1, & \text{若 } i=j,\\ 0, & \text{若 } i\neq j,\end{cases}$$

因此必有(3-2-16)成立。由(3-2-16)即可推得$\Delta(B)\neq 0$的充要条件为B是T型矩阵，若B是T型矩阵，必有

$$\Delta(B)=\Delta_{\alpha_1}(B)=\cdots=\Delta_{\alpha_1\cdots\alpha_{r-1}}(B),$$

且$B_{\alpha_1\cdots\alpha_{r-1}}$是一个$n_{r-1}\times n_{r-1}$阶零矩阵，所以$F_{\alpha_1\cdots\alpha_{r-1}}(B)$是一个$n_{r-1}\times n_{r-1}$阶幺矩阵，$n_{r-1}\geqslant 1$，因此

$$\Delta(B)=\Delta_{\alpha_1\cdots\alpha_{r-1}}(B)=1$$

成立。反之，若$\Delta(B)\neq 0$成立，则记$\alpha_1=\alpha$，且由(3-2-16)知必有一个$\alpha_2\cap\alpha_1=\varnothing$，$\|\alpha_2\|\geqslant 1$，使$B_{\alpha_1}$为一个$(n_1,\alpha_2)$型矩阵。若这样的$\alpha_2$不存在，则$B_{\alpha_1}$的全体列向量均不为零向量，这时必有$F_{\alpha_1}(B)$的行向量之和为零向量，因此

$$\Delta_{\alpha_1}(B)=\|Q_{\alpha_1}(B)\|=0,$$

这与(3-2-16)及假设$\Delta(B)\neq 0$矛盾；若$\alpha_1\cup\alpha_2=N$，则B为T型矩阵；若$\alpha_1\cup\alpha_2\neq N$，同样可证，这时必存在$\alpha_3$，$\|\alpha_3\|\geqslant 1$，$\alpha_3$与$\alpha_1\cup\alpha_2$之交为空集，且$B_{\alpha_1}$为一个$(n_2,\alpha_2)$型矩阵，依次类推，得$B$必为$T$型矩阵，引理得证。

仿照上述引理2中(ii)的讨论，我们同样可得

定理 若B是一个(n,q,α)型矩阵，则$\Delta(B)\neq 0$的充要条件为B是$T_n(q)$型矩阵，这时$\Delta(B)=1$。

若$\|\alpha\|=1$，则$\Delta(B)\neq 1$的充要条件为B是一反树图的联系矩阵，因此寻找$G_n(q)$中的全体反树图，只要寻找$T_n(q)$型矩阵即可。

以下记本节定义 2 中(ii)，(iii) 的 T (或 $T_n(q)$) 型矩阵为

$$T(\alpha_1, \cdots, \alpha_r) \quad (\text{或 } T_n(q; \alpha_1, \cdots \alpha_r))$$

型矩阵。该定理告诉我们，当 $\|\alpha_1\| = 1$ 时，任何 $T_n(q; \alpha_1, \cdots, \alpha_r)$ 型矩阵 B 所相应的图必为 $G_n(q)$ 中的极大反树子图。反之，任何 $G_n(q)$ 图中的极大反树子图的联系矩阵必为 $T_n q; \alpha_1, \cdots, \alpha_r)$型矩阵。

2.3 T 型矩阵的构造与计数

由本节引理 2 中(ii)，我们很快可以构造任意 $n \times n$ 阶 T 矩阵，它的步骤如下：

T_0-Ⅰ 任意选取一组 $\{\alpha_1, \cdots, \alpha_r\}$ 为 $N = \{1, 2, \cdots, n\}$ 的一个分割，此即

$$\alpha_i \cap \alpha_j = \varnothing (\text{若 } i \neq j), \bigcup_{i=1}^{r} \alpha_i = N,$$

且 $\|\alpha_i\| \geqslant 1$, $i = 1, \cdots, r$。以下记

$$i\alpha_i = \{j_{i,1}, \cdots, j_{i,k_i}\}, \ i = 1, \cdots, r. \qquad (3\text{-}2\text{-}17)$$

T_0-Ⅱ 由 $\{\alpha_2, \cdots, \alpha_r\}$ 构造 T 型矩阵 $B = [d_{ij}]$ 如下：

(1) 首先取 $d_{ii} = 0$, $d_{ij} = 0$, 对任何 $i = 1, 2, \cdots, n$, $j \in \alpha_1$。

(2) 记 $\alpha_1^c = N - \alpha_1$, 对任何 $j \in \alpha_1^c$, $i_j \in N$, 使 $d_{i_j j} = 1$, 这时 i_j 是唯一的。我们这样选取，若 $j \in \alpha_k$, $k = 2, \cdots, r$, 则取 $i_j \in \alpha_{k-1}$。

由此得到的 B 矩阵必为 $T(\alpha_1, \cdots, \alpha_r)$ 型矩阵，因为划去 B 中 α_i 的行、列后，α_{i+1} 中的列必为零向量。

例 1 试构造一个 $n = 8$ 的 T 型矩阵。

解 由 T_0-Ⅰ, T_0-Ⅱ，即有

(i) 任取 $N_8 = \{1, \cdots, 8\}$ 的一组分割，如

$$\alpha_1 = \{1, 2\}, \alpha_2 = \{5, 7, 8\}, \alpha_3 = \{4\}, \alpha_4 = \{3, 6\}.$$

(ii) 取 $d_{ii} = 0$, $d_{ij} = 0$, 对任何 $i = 1, 2, \cdots, 8$, $j = 1, 2$。

(iii) 记 i_j, $j = 3, 4, 5, 6, 7, 8$, 为 T_0-Ⅱ 中 (2) 定义的函

数，这时

$$i_5, i_7, i_8 \in \{1, 2\},\ i_4 \in \{5, 7, 8\}, i_3, i_6 \in \{4\},$$

如我们取

$$i_5 = i_8 = 1,\ i_7 = 2,\ i_4 = 8,\ i_3 = i_6 = 4,$$

这时

$$B = \begin{bmatrix} 0&0&0&0&1&0&0&1 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \end{bmatrix}$$

即为所求的 T 型矩阵，易得 $\Delta(B) = 1$。

若记

$\overline{T}(\alpha_1, \cdots \alpha_r) = \{$全体 $T(\alpha_1, \cdots, \alpha_r)$ 型矩阵$\}$，这时显然有计数关系

$$\|\overline{T}(\alpha_1, \cdots, \alpha_r)\| \overset{*}{=} k_1^{k_r} \cdots k_{r-1}^{k_r}, \qquad (3\text{-}2\text{-}18)$$

其中 $k_i = \|\alpha_i\|$, $i = 1, 2, \cdots, r$。

由(3-1-18)可对 T 型矩阵分类作进一步计算，对此不再详述。

2.4 $T_n(q)$型矩阵的构造

在本节的 2.3 段中，我们已给出了一般 T 型矩阵的构造方法，如取 $q = n$ 时，该方法实际上给出了 $G_1(q)$ 图中全体反树的构造方法。现在进一步推广 T_0-Ⅰ，T_0-Ⅱ 的运算步骤，构造 $G_n(q)$ 中的全体反树或全体 $T_n(q)$型矩阵。以下记

$$D_j = \{j \cdot q + i : 0 \leqslant i \leqslant q - 1\}, \qquad (3\text{-}2\text{-}19)$$

其中 $0 \leqslant j \leqslant k_{n-1} = q^{n-1} - 1$。若记

$$B[G_n(q)]=[d'_{ij}]_{q^n\times q^n}$$

$$=\begin{bmatrix} I_n \\ I_n \\ \vdots \\ I_n \end{bmatrix}\Bigg\}q\text{ 个},\qquad (3\text{-}2\text{-}20)$$

其中 I_n 为 (1-5-21) 定义的 $q^{n-1}\times q^n$ 阶矩阵，这时 $d'_{ij}=1$ 的充要条件为

$$j\in D_{j'},\ j'=j(\mathrm{mod}q^{n-1}),\qquad (3\text{-}2\text{-}21)$$

因此，在推广 T_0-Ⅰ，T_0-Ⅲ 的运算时，必需注意条件(3-2-21)。以下我们给出 $T_n(q)$型矩阵的构造运算。

T_0-Ⅰ′ 选取一组 $\{\alpha_1,\cdots,\alpha_r\}$ 为 $F_q^{(n)}=\{0,1,\cdots,k_n\}$ 的一组分割，且满足条件

$$\alpha_{k+1}\subset(\bigcup_{j\in\alpha_k}D_j)\backslash(\bigcup_{i=1}^{k}\alpha_i),\ k=1,\cdots,r-1,\qquad (3\text{-}2\text{-}22)$$

其中 $\alpha\backslash\beta$ 为两集合之差。

T_0-Ⅱ′ 的运算与 T_0-Ⅱ 相同，这时在 T_0-Ⅱ (2)中，对任何 $j\in\alpha_{k+1}$，由 (3-2-22) 知，总有一个 $i_j\in\alpha_k$，使 $j\in D_{i_j}$，因此可取

$$d_{ij}=\begin{cases}1, & \text{若 } i=i_j,\\ 0, & \text{否则},\end{cases}$$

构造的矩阵 B 必为 $B[G_n(q)]$ 的子矩阵，且为 T 型矩阵。

例 2 试构造一个 $T_4(2)$ 型矩阵。

解 利用T_0-Ⅰ′，T_0-Ⅱ′的步骤构造矩阵$B=[d_{ij}]_{16\times16}$如下：

(i) 首先由(3-2-19)知，对任何 $0\leqslant j\leqslant 2^3-1$，可构造

$$D_j=\{2i,\ 2j+1\},\ j=0,1,\cdots,7.$$

(ii) 任取 $\alpha_1=\{0,10\}$，则

$$D_{\alpha_1}=\bigcup_{j\in\alpha_1}D_j=\{0,1,4,5\}.$$

任取 $\alpha_2\subset D_{\alpha_1}$，且

$$\alpha_2=\{1,4,5\},$$

这时由 T_0-Ⅱ′ 可取

$$i_1=0,\ i_4=10,\ i_5=10.$$

(iii) 由 $\alpha_2=\{1,4,5\}$ 得

$$D_{\alpha_2}=\{2,3,8,9,10,11\},$$

任取 $\alpha_3\subset D_{\alpha_2}\backslash(\alpha_1\bigcup\alpha_2)$ 为

$$\alpha_3=\{2,3,11\}.$$

这时，由 T_0-Ⅱ′ 得

$$i_2=i_3=1,\ i_{11}=5,$$

且

$$\alpha_1\bigcup\alpha_2\bigcup\alpha_3=\{0,1,2,3,4,5,10,11\}.$$

(iv) 由 $\alpha_3=\{2,3,11\}$ 得

$$D_{\alpha_3}=\{4,5,6,7,10,11\},$$

取 $\alpha_4\subset D_{\alpha_3}\backslash\{\alpha_1\bigcup\alpha_2\bigcup\alpha_3\}$ 为 $\alpha_4=\{6,7\}$。这时可取 $i_6=3$ 或 11，$i_7=3$ 或 11，我们取

$$i_6=11,\ i_7=3,$$

得到

$$\alpha(4)=\alpha_1\bigcup\cdots\bigcup\alpha_4=\{0,1,\cdots,6,7,10,11\}.$$

(v) 由 $\alpha_4=\{6,7\}$ 得

$$D_{\alpha_4}=\{12,13,14,15\}.$$

若 $\alpha_5=\{13,14,15\}$，则取

$$i_{13}=6,\ i_{14}=i_{15}=7.$$

(vi) 由 $\alpha_5=\{13,14,15\}$得

$$D_{\alpha_5}=\{10,11,12.13,14,15\},$$

则取 $\alpha_6=\{12\}$. $i_{12}=14$，且有

$$D_{\alpha_6}=\{8,9\},$$

这时取 $\alpha_7=\{8,9\}$，$i_8=i_9=12$，即得 $\alpha_1,\alpha_2,\cdots,\alpha_7$ 为 $F_2^{(4)}$ 的一组分割，且由

$$i_1=0,\ i_2=i_3=1,\ i_4=i_5=10,\ i_6=11,\ i_7=3,$$
$$i_8=i_9=12,\ i_{11}=5,\ i_{12}=14,\ i_{13}=6,\ i_{14}=i_{15}=7$$

得相应的 $T_4(2)$型矩阵

$$B=\begin{bmatrix}
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

即为所求。

注意：(1) 在上述 $T_n(q)$ 型矩阵中，若 $\|\alpha_1\|=1$，则相应的 $T_n(q)$型矩阵是 $G_n(q)$ 图中极大反树图的联系矩阵，因此在 T_0-Ⅰ′，T_0-Ⅱ′ 的算法中给出 $\alpha_1=\{x_0\}$ 为单点集，相应的根为 x_0。

(2) 在 T_0-I'，T_0-Ⅱ′ 运算中，若出现

$$\alpha(k)=\bigcup_{i=1}^{k}\alpha_i\neq\hat{N},\ D\alpha_k\backslash\alpha(k)=\varnothing$$

的情形，就要修正 T_0-Ⅰ′，T_0-Ⅱ′ 的算法。取适当 $j\in\hat{N}\backslash\alpha(k)$，

且作

$$\alpha_i' = \alpha_i \cup \{j\},$$

其中 i 为使 $j \in D_{\alpha_{i-1}}$ 成立，然后对 $\alpha_1, \alpha_2, \cdots \alpha_{i-1}, \alpha_i'$ 继续 T_0-Ⅰ′，T_0-Ⅱ′ 的运算即可。

例 3 同样对 $T_4(2)$ 型的情形，按 T_0-Ⅰ′，T_0-Ⅱ′ 算法，可得

$$\alpha_1 = \{0\},\ D_{\alpha_1} = \{0,\ 1\},$$

$$\alpha_2 = \{1\},\ D_{\alpha_2} = \{2,\ 3\},$$

$$\alpha_3 = \{2,\ 3\},\ D_{\alpha_3} = \{4, 5, 6, 7\},$$

$$\alpha_4 = = \{4, 5, 6\},\ D_{\alpha_4} = \{8, 9, 10, 11, 12\},$$

$$\alpha_5 = \{10\},\ D_{\alpha_5} = \{4,\ 5\},$$

则 $D_{\alpha_5} \backslash \alpha(5) = \varnothing$，这时可将

$$N \backslash \alpha(5) = \{7, 8, 9, 11, 12, 13, 14, 15\}$$

中的元补入 α_4，如取

$$\alpha_5' = \{10, 11\ \ 12, 13\}\text{（以下记为 } \alpha_5\text{）},$$

则

$$D_{\alpha_5'} = \{4, 5, 6, 7, 8, 9, 10, 11\}.$$

这时取

$$\alpha_6 = \{7, 8, 9\},\ D_{\alpha_6} = \{14, 15, 0, 1, 2, 3\},$$

$$\alpha_7 = \{14, 15\},\ D_{\alpha_7} = \{8, 9, 10, 11\},$$

其中 $\alpha_1, \cdots, \alpha_7$ 即为所求，且取

$$i_1 = 0,\ i_2 = i_3 = 1,\ i_4 = 2 = i_5,\ i_6 = 3,$$

$$i_7 = 11,\ i_8 = i_9 = 12,\ i_{10} = i_{11} = 5,$$

$$i_{12} = i_{13} = 6,\ i_{14} = i_{15} = 7$$

相应的矩阵 B 为

$$\begin{bmatrix}
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

§3 M-序列的剪接递推构造与密钥空间

3.1 反树图的剪接递推构造

关于反树图的剪接构造，在[2]，[10]中已有详述. 对 $q=2$ 的情形，若记

$$T_0=\{s_0, s_1, \cdots, s_{k_n}\}=\{S_0, S_1, \cdots, S_{k_n}\} \quad (3\text{-}3\text{-}1)$$

为 $G_n(2)$ 中的反干树图，其中 $k_n=2^n-1$，且

$$S_i=(s_{i+1}, s_i),\ i=0, 1, \cdots, k_n$$

为 T_0 中的弧，在(3-3-1)中按相反方向的次序排列。以下记

$$x=(a_1, a_2, \cdots, a_{n-1})\in F_2^{(n-1)}$$

为 F_2 上的 $n-1$ 维向量. 这时

$$S=(z,\ b)\in F_2^{(n)},\ b\in F_2$$

为 $G_n(2)$ 中的状态，记

$$I(z)=\{(a(z,i),\ z,\ b(z,i)),\ i=1,\ 2\} \tag{3-3-2}$$

为 z 在 T_0 中的编号，也就是

$$(a(z,i),\ z,\ b(z,i)),\ i=1,\ 2, \tag{3-3-2a}$$

z 在(3-3-1)的弧 S_i 中第 i 次出现，每个 z 在 S_j 中出现两次. 不失一般性，以下设

$$s_0=(0,\ 0,\ \cdots,\ 0)\in F_2^{(n)} \tag{3-3-3}$$

为 $T_{n,0}$ 的根，这时 $z_0=(0,\ 0,\ \cdots,\ 0)\in F_2^{(n-1)}$，且相应的编号为

$$b(z_0,\ 1)=0,\ b(z_0,\ 2)=1. \tag{3-3-4}$$

同样，记

$$T_{n,0}(i)=\{z,\ b(z,i)),\ z\in F_{2,0}^{(n-1)}\},\ i=1,\ 2. \tag{3-3-5}$$

我们有

定义 记

$$C_{n-1}=\{c(z),\ z\in F_{2,0}^{(n-1)}\} \tag{3-3-6}$$

为 $G_n(z)$ 中反干树的剪接算子，其中

$$c(z)\in F_2,\ F_{2,0}^{(n-1)}=F_2^{(n)}-\{z_0\},$$

这时 C_{n-1} 关于反干树 T_0 的剪接运算为改变 T_0 中的弧，对任何 T_0 中的弧 S 定义

$$C_{n-1}(S)=\begin{cases}(a(z,1),\ z,\ b(z,1)),\ 若\ S=(a(z,1),\\ \qquad z,\ b(z,1))\ 或\ (a(z_0,2),\ z_0,\ b(z_0,2));\\ (a(z,2),\ z,\ b(z,2)+c(z)),\\ 若\ S=(a(z,2),\ z,\ b(z,2)),\ z\in F_{2,0}^{(n-1)},\end{cases} \tag{3-3-7}$$

定理 1 $G_n(2)$ 中全体以 s_0 为根的反树图与全体 $(T_0,\ C_{n-1})$ 1-1 对应，其中 T_0 为 $G_n(2)$ 中任意的反干树，以 s_0 为根，C_{n-1} 为(3-3-6)定义的剪接算子；$c(z)$，$z\in F_{2,0}^{(n-1)}$ 为在 F_2 上取任意值

的参数.

证明　首先对不同的 (T_0, C_{n-1})，得到的反树 $C_{n-1}(T_0)$ 总不相同。因为如果有两个不同的反干树 $T_0 \neq T_0'$，记

$$T_0' = \{s_0', \cdots, s_{in}'\} = \{S_0^n{}', \cdots, S_{kn}'\},$$

则总有一个 $i \geqslant 1$，使

$$s_0 = s_0', \cdots, s_i = s_i', \quad s_{i+1} \neq s_{i+1}'.$$

这时 s_{i+1} 与 s_{i+1}' 的编号必为

$$(z, b(z, 1)) \text{ 与 } (z, b'(z, 1)),$$

其中 $b(z, 1) \neq b'(z, 1)$，且它们的入弧编号相同，即 $a(z, 1) = a'(z, 1)$。而相应于第二组编号为

$$(a(z, 2), z, b(z, 2)) \text{ 与 } (a'(z, 2), z, b'(z, 2)),$$

其中

$$a(z, 2) = a'(z, 2) = a(z, 1) + 1,$$

$$b(z, 2) = b(z, 1) + 1, \quad b'(z, 2) = b'(z, 1) + 1,$$

在 C_{n-1} 运算之后，相应的 4 条弧为

$$(a(z, 1), z, b(z, 1)), \quad (a(z, 2), z, b(z, 2) + c(z)),$$

$$(a'(z, 1), z, b'(z, 1)), \quad (a'(z, 2), z, b'(z, 2) + c(z)).$$

这两组弧互不相同，因此 $C_{n-1}(T_0) \neq C_{n-1}(T_0')$。

若 $T_0 = T_0'$，$C_{n-1} \neq C_{n-1}'$，则 $C_{n-1}(T_0) \neq C_{n-1}'(T_0')$ 是显然的。

反之，对任何反树 T，若 s 是反树 T 中最低层的分权点，这时从 s 到 s_0 点的路上没有 T 的分权点。记 s 的两条入弧为 (t, s)，(t^*, s)，其中 t^* 为 t 的共轭元，这时 s 的相伴元 s' 在反树 T 中必无入弧，因此 s' 为反树 T 的梢点，且必在枝 $T(t, s)$ 或 $T(t^*, s)$ 上，这对我们可作剪接运算

$$(t^*, s) \to (t^*, s') \text{ 或 } (t, s) \to (t, s'),$$

就可消除反树 T 的一个分权点，变反树 T 为反树 T_1。如此继续若干次，就可将反树 T 化为反干树 T_0。可由一个 (3-3-6) 的剪接运算 C_{n-1}，使 $T = C_{n-1}(T_0)$ 成立，且由不同的反树 T 必得不同

的 (T_0, C_{n-1})，定理得证。

推论 $G_n(2)$ 中的全体完备回路，具有固定的起弧 $(s_0, b_0) \in F_2^{(n+1)}$，与本节定理 1 中的 (T_0, C_{n-1}) 相互 1-1 对应，且与 $G_{n+1}(2)$ 中具有确定起点 $(s_0, b_0) \in F_2^{(n+1)}$ 的极大圈相互 1-1 对应。

证明 因为在 $q=2$ 的情形下，$G_n(2)$ 的完备回路 $W(x_0, b_0)$ 与反树图 T 相互 1-1 对应，其中 T 具有根 s_0，由本节定理 1 知，$W(s_0, b_0)$ 与 (T_0, C_{n+1})相互 1-1 对应，它们也与 $G_{n+1}(2)$ 中的极大圈 $M(x_0, b_0)$相互 1-1 对应，命题得证。

以下记 $K_M(n+1) = \{T_{n,0}, C_{n-1}\}$ 为 $G_{n+1}(2)$ 中全体 M-序列的密钥参数，其中 $T_{n,0}$ 为 $G_n(2)$ 中的反干树。

因为 $T_{n,0}$ 为 $G_n(2)$ 中的反干树，它由 $G_n(2)$ 中极大圈除去起弧 (s_0, s_{k_n}) 而得，因此 $T_{n,0}$ 又可由密钥参数

$$K_M(n) = \{T_{n-1,0}, C_{n-2}\}$$

而得，其中 $T_{n-1,0}$ 为 $G_{n-1}(2)$ 中的反干树，$C_{n-2} = \{c(z), z \in F_{2,0}^{(n-1)}\}$ 为 $G_{n-1}(2)$ 中反剪接算子。依次类推，我们可得到一系列

$$K_M(t) = \{T_{t-1,0}, C_{t-2}\},\ t = 3, 4, \cdots, n+1$$

密钥参数，若记

$$C_t = \{c_{ti}, i = 1, 2, \cdots, k_t\},\ c_{ti} \in F_2, \tag{3-3-8}$$

其中 $k_t = 2^t - 1$。又记

$$K_M(n+1) = \begin{bmatrix} c_{11} & & & \\ c_{21} & c_{22} & c_{23} & \\ c_{31} & c_{32} & \cdots & c_{37} \\ \cdots\cdots & & & \\ c_{n-1,1} & c_{n-1,2} & \cdots c_{n-1} & k_{n-1} \end{bmatrix} \tag{3-3-9}$$

为 $G_{n+1}(2)$ 中全体 M-序列的密钥参数空间，这样当起点

$$(s_0, b_0) = (0, 0, \cdots, 0, 0) \in F_2^{(n+1)} \tag{3-3-10}$$

及由 $G_2(2)$ 上的反干树

$$T_{2,0} = \{(00) \leftarrow (10) \leftarrow (11) \leftarrow (01)\} \tag{3-3-11}$$

给定后，全体 $M_{n+1}(g)$-序列与 $K_M(n+1)$就 1-1 对应。这时，(3-3-11)的 $T_{2,0}$是 $G_2(2)$ 中唯一的反干树(以 (00) 为 根)。以下我们记

$$\begin{aligned}\widetilde{K}_M(n+1) = \{&\text{全体 (3-3-9) 的 } K_M(n+1),\\ &\text{其中 } c_{ij} = 0 \text{ 或 } 1,\ i = 1, \cdots, n-1,\ j = 1, \cdots, k_i\},\end{aligned} \tag{3-3-12}$$

这时有

定理 2 若 (3-3-10) 在起始点固定条 件 下 $\widetilde{M}(s_0, n+1, 2)$ 与 (3-3-12) 的 $\widetilde{K}_M(n+1)$ 空间 1-1 对应，则任何 $\widetilde{M}(s_0, n+1, 2)$ 中的元可按本节定理 1 的剪接递推规则，由 $T_{2,0}$及 $\widetilde{K}_M(n+1)$中的元 $K_n(n+1)$ 唯一确定。这里取

$$S_0 = (s_0, b_0) = (0, 0, \cdots, 0, 0) \in F_2^{(n+1)}.$$

该定理的证明由上述讨论已可以说明，因为 $T_{2,0}$及 $K_n(n+1)$ 可依次

由 $T_{2,0}$, C_1 确定 M_3, $T_{3,0}$;

由 $T_{3,0}$, C_2 确定 M_4, $T_{4,0}$;

……

由 $T_{n,0}$, C_{n-1} 确定 M_{n+1} 为所求。

其中 M_t 为 $G_t(2)$ 中的极大圈。反之，

由 M_{n+1} 确定 W_n, $T(W_n)$, $T_{n,0}$, C_{n-1};

由 $T_{n,0}$ 确定 W_{n-1}, $T(W_{n-1})$, $T_{n-1,0}$, C_{n-2};

……

由 $T_{3,0}$ 确定 W_2, $T(W_2)$, $T_{2,0}$, C_1。

其中 W_t 为 $G_t(2)$ 中的完备回路，$T(W_t)$ 为由 W_t 确 定 的 反 树 图，因此由 M_{n+1} 唯一确定 $K_M(n+1) \in \widetilde{K}_M(n+1)$。这时显然有

$$\|\widetilde{K}_M(n+1)\| = 2^{2^n-(n+1)} = M(n,2) \qquad (3\text{-}3\text{-}13)$$

成立。

例 取 $n=4$，在 (3-3-10) 初始条件下，由

$$K_4(5) = \begin{bmatrix} 1 & & & & & & & \\ 0 & 1 & 0 & & & & & \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & \end{bmatrix},$$

求 $G_5(2)$中由 $K_4(5)$ 产生的 M-序列。

解 由本节定理 2 的步骤求 $G_2(2)$ 中的M-序列步骤如下：

(1) $G_2(2)$ 中唯一的反于树为

$$T_{2,0}=\{(00)\leftarrow(10)\leftarrow(11)\leftarrow(01)\}。$$

由 $C_1(T_{2,0})$ 得反树

$$T_2=\left\{(00)\leftarrow(10)\begin{matrix}\swarrow(11)\\ \nwarrow(01)\end{matrix}\right\}。$$

因为 C_1 关于弧 (011) 的运算为

$$C_1(011)=(0,1,1+c_{11})=(010),$$

由 T_2 决定的完备回路为

$$W_2=\{00\to00\to01\to11\to11\to10\to01\to10\to00\},$$

相应于 $G_3(2)$ 中的极大圈为

$$M_3=\{000\to001\to011\to111\to110\to101\to010\to100\to000\}。$$

(2) 由 M_3 决定 $G_3(2)$ 中反于树为

$$T_{3,0}=\{000\leftarrow100\leftarrow010\leftarrow101\leftarrow110\leftarrow111\leftarrow011\leftarrow001\},$$

由 C_2 对 $T_{3,0}$ 的弧进行剪接的运算知

$$C_2(1101)=(1,1,0,1+c_{21})=(0011),$$
$$C_2(0011)=(0,0,1,1+c_{22})=(0010),$$
$$C_2(0111)=(0,1,1,1+c_{23})=(0111)。$$

这时由 $C_2(T_{3,0})$ 为

$$T_3=\{000\leftarrow100\leftarrow010\leftarrow101\leftarrow110\leftarrow111\leftarrow011\}\begin{matrix}\swarrow001\end{matrix},$$

相应的完备回路为

$$W_3=\{000\to000\to001\to011\to110\to100\to001\to010\to101\to011\to111\to110\to101\to010\to100\to000\},$$

$G_4(2)$ 中的极大圈与反干树为

$$M_4=\{0000\to0001\to0011\to0110\to1100\to1001\to0010\to0101\to1011\to0111\to1111\to1110\to1101\to1010\to0100\to1000\to0000\},$$

$$T_{4,0}=\{0000\leftarrow1000\leftarrow0100\leftarrow1010\leftarrow1101\leftarrow1110\leftarrow1111\leftarrow0111\leftarrow1011\leftarrow0101\leftarrow0010\leftarrow0010\leftarrow1100\leftarrow0110\leftarrow0011\leftarrow0001\}.$$

(3) 由 C_3 对 $T_{4,0}$ 的弧进行剪接运算，得

$C_3(11001)=(11000)$，$C_3(00101)=(00100)$，

$C_3(01100)=(01101)$，$C_3(00011)=(00011)$，

$C_3(01011)=(01010)$，$C_3(00110)=(00111)$，

$C_3(01111)=(01110)$.

这时由 $C_3(T'_{4,0})$ 得

$$T_4=\left\{0000\leftarrow\begin{array}{c}1001\qquad\qquad\qquad\qquad0001\\ 1100\ \ 0010\ \ 0101\ \ 0110\ \ 1111\ \ 0011\\ \leftarrow1000\leftarrow0100\leftarrow1010\leftarrow1101\leftarrow1110\leftarrow0111\leftarrow1011\end{array}\right\},$$

从而得

$$W_4=\{0000\to0000\to0001\to0010\to0101\to1011\to0110\to1100\to1001\to0011\to0110\to1101\to1011\to0111\to1111\to1111\to1110\to1100\to1000\to0001\to0011\to0111\to1110\to1101\to1010\to0101\to1010\to0100\to1001\to0010\to0100\to1000\to0000\},$$

$$M_5=\{00000\to00001\to00010\to00101\to\to01011\to10110$$

→01100→11001→10011→00110→01101→11011
→10111→01111→11111→11110→11100→11000
→10001→00011→00111→01110→11101→11010
→10101→01010→10100→01000→10000→00000}

即为所求。

以下我们称 $\widetilde{K}_M(n+1)$ 为 $G_{n+1}(2)$ 中全体M-序列的剪接递推密钥空间，相应的元 $K_M(n+1)$ 为 $M_{n-1}(2)$-序列的剪接递推算子，由参数 c_{ij}，$i=1,\cdots,n-1$，$j=1,\cdots k_{n-1}$ 决定。

3.2 M-序列的剪接递推公式

在例题中，我们已给出了由 $M_n(2)$-序列的剪接密钥参数 $K_M(n+1)$ 构造 $M_{n+1}(2)$-序列的过程，现在进一步讨论它的一般递推公式。

设 $T_{n,0}$ 为(3-3-1)中 $G_n(2)$的反干树图，如果增加弧(s_0,s_{k_n})，则 $T_{n,0}$ 就变为 $G_n(2)$中的极大圈 M_n。我们记

$$(a(z,i),z,b(z,i)),\ i=1,2,\ z\in F_2^{(n-1)} \tag{3-3-14}$$

为 $T_{n,0}$ 中出入弧的编号，这时(3-3-14) 的弧为 $(z,b(z,i))$ 的入弧及 $(a(z,i),z)$ 的出弧，其中 i 为 z 在 $T_{n,0}$ 中出现的次数。由(3-3-17)给出了 C_{n-1} 对 $T_{n,0}$的剪接运算，我们记之为 $C_{n-1}(a(z,j),z,b(z,i))$，从而得到反树图

$$T_n=\{F_2^{(n)},\ C_{n-1}(T_{n,0})\}, \tag{3-3-15}$$

其中

$$C_{n-1}(T_{n,0})=\{C_{n-1}(a(z,i),z,b(z,i)):i=1,2,z\in F_2^{(n-1)}\}, \tag{3-3-16}$$

按 $M_{n+1}(2)$-序列的构造步骤，由 T_n 即可产生 $G_n(2)$ 中完备回路

$$\begin{aligned}W_n(T_n)&=\{s_0,s_1,\cdots,s_{k^{n+1}}\}\\&=\{S_0,S_1,\cdots,S_{k^{n+1}}\},\end{aligned} \tag{3-3-17}$$

其中 S_i(或 S_i) 的次序排列沿弧的方向，而起弧 $S_0=(0,0,\cdots,0,0)\in F_2^{(n+1)}$。这时对每个

$$s=(a_0, a_1, \cdots, a_{n-1})\in F_2^{(n)},$$

在 $W_n(T_n)$ 中出两次，同样可有出入弧的编号为

$$(a(s,i), s, b(0,i)), i=1, 2, s\in F_2^{(n)}. \qquad (3\text{-}3\text{-}18)$$

由 W_n 的构造过程知，(3-3-18) 的弧满足以下关系式：

$$b(s,1)=\bar{b}(s,2)=1+b(s,2), \qquad (3\text{-}3\text{-}19)$$

$$b(s,2)=\begin{cases} b(z,1), & \text{若 } s=(a(z,1),z), \\ b(z,2)+c_{n-1}(z), & \text{如 } s=(\bar{a}(z,1),z), \end{cases} \qquad (3\text{-}3\text{-}20)$$

其中 $(a(z,i), z, b(z,i))$ 为反树 $T_{n,0}$ 的编号。由 (3-3-14) 定义，且

$$C_{n-1}=(c_{n-1}(z), z\in F_{2,0}^{(n-1)})$$

为剪接算子(即 $c_{n-1}(z)=c_{n-1,z}$ 由 (3-3-6)或 (3-3-9) 定义)。另外，由 s 的编号定义直接可得关系式

$$a(s,1)=\bar{a}(s,2)=1+a(s,2) \qquad (3\text{-}3\text{-}21)$$

成立。

我们称 (3-3-19)～(3-3-21)为 M-序列的剪接递推公式。由这些公式，可直接从 $M_n(2)$-序列的编号与剪接算子 C_{n-1} 写出 $M_{n+1}(2)$-序列的全体出弧编号，从而完全确定 $M_{n+1}(2)$-序列。

注意：(1) 在以上记号中，我们虽然对回路 W_n 与反干树 $T_{n,0}$ 的编号作了不同的定义，它们的次序分别按弧的正、反方向规定，但无本质区别，只要交换一下编号次序即可一致。有时为了表达方便，我们仍保持不同的定义。

(2) 在递推式(3-3-19)～(3-3-21)中，可由 $T_{n,0}$ 与 C_{n-1} 可直接写出 W_n 的出弧编号，因此可完全确定 W_n 或 M_{n+1}，从而使 W_n 中入弧的编号 $(a(s,i), s)$ 也完全确定。但我们还没有得到 $a(s,i)$ 的直接表示式，因此不能说 $M_n(2)$-序列的构造问题已完全解决，有兴趣的读者可继续考虑这个问题。这个问题的解决，可使我们对 $M_n(2)$-序列的构造有一个比较全面而彻底的认识。

§4 M-序列剪接构造中的组合表示

4.1 概述

在本章§2、§3中，我们已介绍了两种关于M-序列的构造方法，它的基本思路是给出一个能够表示全体$M_n(q)$-序列的参数空间，及由相应参数确定$M_n(q)$-序列的算法。因为该参数空间与全体$M_n(q)$-序列具有1-1对应的特征，因此§2、§3可看作M-序列构造中的规范化处理。

正如§3所指出的那样，在§3中虽然表示全体$M_n(2)$-序列的密钥参数$K_M(n)$具有简单而明确的意义，但由$K_M(n)$构造$M_n(2)$-序列的过程是一个递推过程，必需逐次计算$M_i(2)$-序列，$i=2,3,\cdots,n$。这不仅对$M_n(2)$-序列的构造过程增加复杂性，也有碍于我们对M-序列构造的进一步认识。本节试图进一步讨论关于M-序列在剪接构造中的组合表示与性质，有关结论对寻找M-序列及它们的函数表示形式能起到一定程度的简化作用。

4.2 M-序列的组合表示

对$q=2$的情形，在本章§1中已指出，非奇异函数

$$f(x^{(n)})=x_1+f_0(x_2,\cdots,x_n) \tag{3-4-1}$$

等价于$f(x^{(n)})$的组合表示向量

$$\tilde{\tau}(n)=(\tau_z, z\in F_2^{(n-1)}),\ \tau_z\in F_2. \tag{3-4-1α}$$

它们在

$$A_0[f(x^{(n)})]=\{(\tau_z, z): z\in F_2^{(n-1)}\} \tag{3-4-2}$$

或

$$A_0[f_0(x_2,\cdots,x_n)]=\{z=(x_2\cdots,x_n):\tau_z=0\} \tag{3-4-2α}$$

的意义下，$f(x^{(n)})$与$\tilde{\tau}(n)$ 1-1对应，因此在下文中，我们把(3-4-1)的$f(x^{(n)})$与$\tilde{\tau}(n)$同时称为非奇异函数。

以下记M_n为$G_n(2)$中的一个M-序列，在§3中我们已给

出了它的编号定义为

$$(a(z, i), z, b(z, i)), i=1, 2, z\in F_2^{(n-1)}, \quad (3-4-3)$$

其中规定 $S_0=(0, 0, \cdots, 0)\in F_2^{(n)}$ 为 M_n 的起点。(3-4-3)中的 i 为 z 在 $M_n(2)$ 中出现的次序，而 $(a(z, i), z, b(z, i))$ 为相应于 z 在第 i 次出现时的弧，这时，$M_n(2)$ 的组合表示为

$$\tau_z=\begin{cases} a(z, i), & \text{若 } b(z, i)=0, \\ \bar{a}(z, i), & \text{若 } b(z, i)=1. \end{cases} \quad (3-4-4)$$

因为在非奇异函数中的弧具有共轭且相伴性，即

$$(a(z, 1), b(z, 1))=(\bar{a}(z, 2), \bar{b}(z, 0)), \quad (3-4-4a)$$

因此 (3-4-4) 中的 τ_z 与 i 无关。以下记

$$Q_n=\{s_0, s_1, \cdots, s_k\}$$

为 $G_n(2)$ 中的任一个圈，其中 (s_t, s_{t+1}) 为将 s_t 相连的弧，我们称

$$Q_n^+=\{(s_0, s_1), (s_1, s_2), \cdots, (s_k, s_0)\}$$

为 Q_n 的一个扩张，显然这时 Q_n^+ 是 $G_{n-1}(2)$ 中的圈。

若 M_n 为 $G_n(2)$ 中的极大圈(M-序列)，则 M_n^+ 为 $G_{n+1}(2)$ 中的圈，若记 (3-4-3) 中的弧段为

$$z=(a_1, \cdots, a_{n-1}), z'(z, i)=(a_2, \cdots a_{n-1}, b(z, i)),$$
$$z''(z, i)=(a(z, i), a_1, \cdots, a_{n-2}), \quad (3-4-5)$$

且记

$$(e(z, i), z''(z, i)), (z'(z, i), e'(z, i)) \quad (3-4-6)$$

为 $(a(z, i), z, b(z, i))$ 的入弧与出弧，这时显然有关系式

$$e(z, i)=\begin{cases} \tau_{z''(z, i)}, & \text{若 } a_{n-1}=0, \\ \bar{\tau}_{z''(z, i)}, & \text{若 } a_{n-1}=1; \end{cases} \quad (3-4-7)$$

$$e'(z, i)=\begin{cases} 0, \text{若 } a_1=\tau_{z'(z, i)}, \\ 1, \text{若 } a_1\neq\tau_{z'(z, i)}. \end{cases} \quad (3-4-7a)$$

成立。以下记 $s=(a_1, \cdots, a_n)\in F_2^{(n)}$ 为 $F_2^{(n)}$ 的状态，且记

$$\tau_s=\begin{cases} a(z,i), & \text{若 } s=(z,b(z,i)) \text{ 且 } e'(z,i)=0,\\ \bar{a}(z,i), & \text{若 } s=(z,b(z,t)) \text{ 且 } e'(z,i)=1. \end{cases} \tag{3-4-8}$$

这时有

引理 1 $\tilde{\tau}(n+1)=(\tau_s, s\in F_2^{(n)})$ 为 $M_n^*(2)$-序列的组合表示，即有关系式

$$A_0^{(n+1)}[M_n^*(2)]=\{(\tau_s, s), s\in F_2^{(n)}\} \tag{3-4-9}$$

成立，其中 $A_0^{(n+1)}[M_n^*(2)]$为 $G_{n+1}(2)$中周期序列 $M_n^*(2)$的组合表示，且 (3-4-8) 满足关系式

$$\tau_s=\begin{cases} e(z,i), & \text{若 } s=(a(z,i),z), \text{且 } a_{n-1}=0,\\ \bar{e}(z,i), & \text{若 } s=(a(z,i),z,), \text{且 } a_{n-1}=1. \end{cases} \tag{3-4-10}$$

证明 对任何 $s\in F_2^{(n)}$，我们总可找到一个 $z\in F_2^{(n-1)}$ 与 $b(z,i)\in F_2$，使 $s=(z,b(z,i))$成立。因为在 $M_n^*(2)$ 图中，$(a(z,i),s)$为 $M_n^*(2)$ 上的点，相应的出弧为$(a(z,i),s,e'(z,i))$，因此 $e'(z,i)=0$ 的充要条件为 $a(z,i)=\tau_s$，此即证得 (3-4-9) 成立。对于 (3-4-10)，只要将 $s=(a(z,i),z)$ 代入 (3-4-8) 即得，引理得证。

由这个引理确定了 $G_n(2)$ 中极大圈扩张在 $G_{n+1}(2)$ 中的组合表示。以下引理说明了 $G_n(2)$ 与 $G_{n+1}(2)$ 中两个极大圈之间的关系。

引理 2 若 $M_n(2)$ 为 $G_n(2)$中的极大圈，$M_n^*(2)$ 为 $M_n(2)$的扩张，则

$$(a(s,j),s,b(s,j)),\ j=1,2,\ s\in F_2^{(n)} \tag{3-4-11}$$

为 $M_{n+1}(2)$-序列的编号，其中

$$a(s,2)=e(z,i),\ b(s,2)=\bar{b}(z,i). \tag{3-4-12}$$

当 $s=(a(z,i),z)$ 时，且

$$(a(s,1),b(s,1))=(\bar{a}(s,2),\bar{b}(s,2)). \tag{3-4-13}$$

(3-4-12) 又可表示

$$a(s, 2) = a(z, i), b(s, 2) = e'(z, i),$$

当 $s = (z, b(z, i))$ 时。

该引理告诉我们，如把 M_n^* 的弧作为 M_{n+1} 的第二编组的弧，与 M_n^* 共轭且相伴的弧作为 M_{n+1} 的第一编组的弧，则 M_{n+1} 必为 $G_{n+1}(2)$ 为上的M-序列。

证明 该引理的证明由 M_{n+1} 的构造过程即得，这实际上是把反干树 $T_{n,0}$ ($T_{n,0}$ 为由 M_n 产生的反干树)的弧及弧

$$(s_0, 1) = (0, 0, \cdots, 0, 1) \in F_2^{(n+1)},$$

作为 M_n 的第二组编号的弧，其中 W_n 为由反干树 $T_{n,0}$ 产生的 $G_n(2)$ 完备回路，因此由本引理定义的 M_{n+1} 为 $G_{n+1}(2)$ 中的 M-序列，所以 (3-4-11)～(3-4-13) 成立。引理得证。

上面证明中的完备回路 W_n 还可有更多的性质，如 $G_n(2)$ 中极大圈 M_n 的全体弧由 (3-4-2) 定义，则我们记 M_n^c 为全体弧

$$(a(z, i), z, \bar{b}(z, i)), z \in F_2^{(n-1)}, i = 1, 2 \qquad (3\text{-}4\text{-}14)$$

的集合。这时有

引理 3 由 (3-4-14) 定义的 M_n^c 中全体

$$F_{2,1}^{(n)} \triangleq F_2^{(n)} - \{(0, 0, \cdots, 0), (1, 1, \cdots, 1)\} \qquad (3\text{-}4\text{-}15)$$

的点连成几个圈。

证明 因为在 (3-4-14) 的弧中，对固定的 z，由

$$(a(z, 1), z, \bar{b}(z, 1)) = (\bar{a}(z, 2), z, b(z, 2))$$

知弧 $(a(z, i), z), \rightarrow (z, \bar{b}(z, i))$ 是 1-1 对应的，因此 M_n^c 由若干圈构成，且环

$$(0, 0, \cdots, 0) \rightarrow (0, 0, \cdots, 0), (1, 1, \cdots, 1) \rightarrow (1, 1, \cdots, 1) \qquad (3\text{-}4\text{-}16)$$

在 M_n^c 中。引理得证。

以下记 $Q_i, i = 0, 1, \cdots, k$ 为 M_n^c 中的全体圈，s_i 为 Q_i 中的元在 M_n 中排列最前的点，我们称 s_i 为 Q_i 的首元。记 (3-4-15) 中的两个圈为 Q_0, Q_k，这时

$$S_0=(0,0,\cdots,0),\quad S_k=(1,1\cdots,1).$$

定理 1 如记 $\tilde{\tau}'(n+1)=(\tau'_s, S\in F_2^{(n)})$ 为由 (3-4-8)定义的及 M_n^* 确定的组合表示。这时，$\tilde{\tau}(n+1)=(\tau_s, S\in F_2^n)$为由 M_n 确定的 M_{n+1} 序列，其中

$$\tau_s=\begin{cases}\tau_s, & \text{若 } s\in\{s_0,\cdots,s_k\},\\ \bar{\tau}_s, & \text{否则},\end{cases}\tag{3-4-17}$$

其中 S_i 为 Q_i 的首元。

证明 如图 3-1 所示，大圆为 M_n 的弧，两个小圆与多边形为 M_n^c 中的弧，这时，完备回路 W_n 的走向分别沿 M_n 或 M_n^c 的弧延伸。若所到达的点 s 不在 $\{s_0, s_1, \cdots, s_k\}$ 中，那么 W_n 所引的弧继续在原 M_n 或 M_n^c 中延伸；若 s 为 s_i, $i=0,\cdots,k$ 的点，则 W_n 延伸的弧必改变方向，从 M_n (或 M_n^c) 移向 M_n^c (或 M_n)，因此必有 (3-4-17) 成立，定理得证。

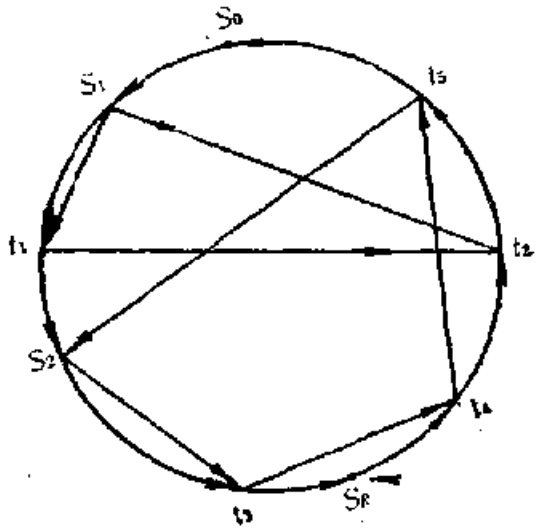


图 3-1 $G_n(2)$ 中完备回路图

例 1 已知

$M_{3,1}=\{000\to001\to011\to111\to110\to101\to010\to100\to000\}$,

$M_{3,2}=\{000\to001\to010\to101\to011\to111\to110\to100\to000\}$,

为 $G_2(2)$ 中的两个极大圈，求由 $M_{3,1}$, $M_{3,2}$ 确定的 $G_4(2)$ 中两个极大圈 $M_{4,1}$, $M_{4,2}$。

解 对此我们分以下几步讨论。

(1) 由 (3-4-10) 写出 $M_{3,1}^*$, $M_{3,2}^*$ 的组合表示

$$\tilde{\tau}'(4)=(\tau'_{000},\tau'_{100},\tau'_{010},\tau'_{110},\tau'_{001},\tau'_{101},\tau'_{011},\tau'_{111}),\tag{3-4-18}$$

它们分别为向量

(0, 0, 1. 0, 1, 1 1, 0), (0, 1, 1, 1, 0, 1, 0, 0)。

(2) $M_{3,1}^{*}$, $M_{3,2}^{*}$ 中的圈除了(3-4-15)的两个环之外分别有:

$Q_{1,1}=\{001\to010\to101\to011\to110\to100\to001\}$,

$Q_{2,1}=\{001\to011\to110\to101\to010\to100\to001\}$,

它们具有相同的三个首元为 (0, 0, 0), (1, 1, 1), (0, 0, 1)。

(3) 由 (3-4-17) 得到 $M_{4,i}$, $i=1, 2$ 的组合表示 $\tau(4)=(\tau_z, z\in F_2^{(3)})$,它们分别为向量

(1, 0, 1, 0, 0, 1, 1, 1), (1, 1, 1, 1, 1, 0, 1)。 (3-4-19)

其中各向量的排列次序与 (3-4-18) 相同。

由 (3-4-19) 的两个 $\tau(4)$产生的 $M_{4,i}$ 序列分别为

$$M_{4,1}=\{0000\to0001\to0010\to0101\to1011\to0110\to1100\to1001\to0011\to0111\to1111\to1110\to1101\to1010\to0100\to1000\to0000\},$$

$$M_{4,2}=\{0000\to0001\to0011\to0110\to1101\to1010\to0100\to1001\to0010\to0101\to1011\to0111\to1111\to1110\to1100\to1000\to0000\}。$$

该例中的构造过程说明本节定理 1 的正确性。

4.3 在剪接密钥作用下的序列的组合表示

在 4.2 段中，我们已给出了由 $G_n(2)$ 中极大圈 M_n 产生 $G_{n+1}(2)$ 中极大圈 M_{n+1} 的计算过程，以及它们的组合表示。现在进一步考虑在 § 3 的剪接密钥作用下产生的 $M_{n+1}(2)$-序列及它们的组合表示。设

$$C_{n-1}=(c_{n-1,1}, c_{n-1,2}, \cdots, c_{n-1}, k_{n-1})$$

为 (3-3-6) 给定的剪接算子，为简起见，以下记 $c_z=c_{n-1,z}$, $z\in F_2^{(n-1)}$,这时 C_{n-1} 对 M_n 作用为使 M_n 的弧$(a(z, i), z, b(z,i))$变为

$$C_{n-1}[(a(z, t), z, b(z, i)]$$

$$=\begin{cases}(a(z,i),z,b(z,i)), & \text{若 } i=2 \text{ 或 } z=0,\\ (a(z,i),z,b(z,i)+c_z), & \text{若 } i=1,z\neq 0.\end{cases}$$

(3-4-20)

全体(3-4-20)的弧为 $C_{n-1}(M_n)$，若切除 $C_{n-1}(M_n)$ 中的起弧 $(a(z_0,1),z_0,b(z_0,1))$ $(z_0=(0,0,\cdots,0)\in F_2^{(n-1)})$，这时 $C_{n-1}(M_n)$ 为反干树。以下记

$$C_{n-1}(M_n)^c=\{(a'(z,i),z,b'(z,i));$$
$$(a'(z,i),z,\bar{b}'(z,i))\in C_{n-1}(M_n)\},\quad (3\text{-}4\text{-}21)$$

因为 C_{n-1} 的作用，使 M_n 与 M_n^c 均发生变化。因为 $c_z=0$ 或 1，若 $c_z=0$，则由(3-4-20)知

$$C_{n-1}[(a(z,i),z,b(z,i)]=(a(z,i),z,b(z,i)),$$

所以我们称 M_n 在 z 处发生了剪接。若 $c_z=1$，以下证明中只考虑发生剪接的点。

另一方面，由4.2段的讨论知，M_n^c 由若干圈 $Q_0,Q_1,\cdots,Q_t$ 构成，它们的全体弧为

$$(a(z,i),z,\bar{b}(z,a)),\ i=1,2,\ z\in F_2^{(n-1)}.\quad (3\text{-}4\text{-}22)$$

因为在剪接运算中，只对 $i=1$ 的弧进行剪接，因此对任何 $z\in F_2^{(n-1)}$，必有且只有一个 Q_t，使

$$(a(z,1),z,\bar{b}(z,1))\in Q_t,$$

这时我们称 $z\in Q_t$，且若 $(a(z,1),z)$ 为 Q_t 的首元，记 M_n^c 中过 z 点的圈为 Q_t，相应的弧为

$$(s,t)=(a(z,1),z,b(z,1)),\ (s,t')=(a(z,1),z,\bar{b}(z,1)),$$

(3-4-23)

其中 $(s,t')\in Q_t$，$(s,t)\in M_n$。又记

$$s(z)=\{s,t,t'\},\quad (3\text{-}4\text{-}24)$$

我们称 $s(z)$ 中的点 v 为变动点。如 $C_z=1$ 且在 Q_t 的图中，则经 C_{n-1} 在 z 点处剪接后，v 点的出入弧中有一条发生变化。$s(z)$ 中的变动点集合记为 $S_0(z)$。

同样，我们可以两个定义点 z_1, z_2 的变动点。如记 s_i, t_i, t_i' 为 (3-4-23) 中当 $z=z_i$ 的点，而

$$s(z_1, z_2)=\{s_1, t_1, t_1', s_2, t_2, t_2'\}. \qquad (3-4-24a)$$

也可以定义 $s(z_1, z_2)$中的变动点，如 $c_{z_1}=c_{z_2}=1$，且 $v\in s(z_2, z_2)$ 的点有一条出，入弧发生变化。

全体 $s(z_1, z_2)$ 中的变动点为 $S_0(z_1, z_2)$，这样我们可以得到 C_{n-1} 的变动点为

$$S_0(C_{n+1})=S_0(z: c_z=1), \qquad (3-4-24b)$$

即是使 $c_z=1$ 的全体 z 的变动点。如果记

$$\tau(n+1)=(\tau_s, s\in F_2^{(n)}),\ \tau'(n+1)=(\tau'_s, s\in F_2^{(n)}),$$

分别为由 M_n, $C_{n-1}(M_n)$ 产生的 M-序列的组合表示，则必有

$$\tau_s'=\begin{cases}\tau_s, & \text{若 } s\notin S_0(C_{n-1}),\\ \bar{\tau}_s, & \text{若 } s\in S_0(C_{n-1}).\end{cases} \qquad (3-4-25)$$

于是，由 M_{n+1} 的组合表示可给出 C_{n-1} 剪接下产生 M-序列 的组合表示。

例 2 求例 1 中序列 $-M_n=M_{n,1}$ 在剪接算子 C_{n-1} 作用下产生的 M-序列。

解 (1) 在例 1 中，序列$-M_{3,1}$ 产生的 $M_{4,1}$-序列的组合表示由 (3-4-19) 给定为

$$\bar{\tau}_0(4)=(1, 0, 1, 0, 0, 1, 1, 1).$$

M_n^c 由 (3-4-16) 的两个环与下面的圈构成：

$$Q_{4,0}=\{001\to010\to101\to011\to110\to100\to001\}.$$

(2) 全体 $C_2=(c_{10}, c_{01}, c_{11})$ 运算记为 $c_{2,i}$, $i=0.1, \cdots, 7$，按 $i\overset{*}{=}c_{10}+2c_{01}+2\cdot c_{01}+2^2c_{11}$ 的编号排列为

$$(0, 0, 0),\ (1, 0, 0),\ (0, 1, 0),\ (1, 1, 0),$$
$$(0, 0, 1),\ (1, 0, 1),\ (0, 1, 1),\ (1, 1, 1).$$

这时 $Q_{4,0}$ 在 $c_{2,i}$, $i=1, \cdots, 7$ 的剪接下变为

$$Q_{4,1}=\{001\to010\to110\to100\to001\to010\to101\},$$

$Q_{4,2}=\{001\to010\to101\to011\to110\to101\to010\to100\to001\}$,

$Q_{4,3}=\{001\to011\to110\to101\to011\to111\to110\to100\to001\}$,

$Q_{4,4}=\{001\to010\to101\to011\to111\to111\to110\to100\to001\}$,

$Q_{4,5}=\{001\to011\to111\to111\to110\to100\to001\to010\to101$
$\to011\}$,

$Q_{4,6}=\{001\to010\to101\to011\to111\to111\to110\to101$
$\to011\to110\to100\to001\}$,

$Q_{4,7}=\{001\to011\to111\to111\to110\to101\to011\to110$
$\to100\to011\to010\}$,

相应的变动点 $S_0(c_{2,i})$, $i=1,\cdots,7$ 为

$\{(001),(011)\}$, $\{(110),(100)\}$,

$\{(001),(011),(110),(101)\}$, $\{(011),(110)\}$

$\{(001),(110)\}$, $\{(011),(101)\}$, $\{(001),(101)\}$,

从而得到由 $C_{n-1}(M_{2,1})$ 产生的 M-序列为：

$\tilde{\tau}_1(4)=(10101101)$, $\tilde{\tau}_2(4)=(11110111)$,

$\tilde{\tau}_3(4)=(10111001)$, $\tilde{\tau}_4(4)=(10110101)$,

$\tilde{\tau}_5(4)=(10101101)$, $\tilde{\tau}_6(4)=(10100001)$,

$\tilde{\tau}_7(4)=(10101011)$.

这个计算过程较本章 §3 的过程有一定的简化。

4.4 由非奇异函数扩张产生的 M-序列

首先，在本节 4.2 段中给出的关于 $G_n(2)$ 中极大圈扩张及其组合表示的有关论述，均可推广到一般非奇异函数情形。如 $\tilde{\tau}(n)$ 为非奇异函数，则我们可由 (3-4-3)～(3-4-8) 构造 $G_n(2)$, $G_{n+1}(2)$ 中的弧及相应的 $\tilde{\tau}(n+1)$。

定义 1 (i) 一个非奇异函数 $\tilde{\tau}(n)$，若它的图中含有 $S_0\to S_0$ ($S_0=(0,0,\cdots,0)$) 环，则称 $\tilde{\tau}(n)$ 为含零环的，否则为非含零环的。

(ii) 两个非奇异函数

$$\tilde{\tau}(n)=(\tau_z,\ z\in F_2^{(n-1)}),\quad \tilde{\tau}'(n)=(\tau'_z,\ z\in F_2^{(n-1)})$$

称为互补的，若对任何 $z\in F_2^{(n-1)}$，$\tau'_z=\bar{\tau}_z$ 成立。

以下称由 (3-4-9) 定义的 $\tilde{\tau}(n+1)$ 为由 $\tilde{\tau}(n)$ 产生的非奇异函数，并且记为 $\tilde{\tau}(n+1)=\tilde{\tau}(n)^*$。显然，我们注意到互补的 $\tilde{\tau}(n)$ 与 $\tilde{\tau}'(n)$，它们产生的 $\tilde{\tau}(n+1)$ 与 $\tilde{\tau}'(n+1)$ 一般不具有互补性。另外，显然有 $\tilde{\tau}(n)$ 为含零环的充要条件是 $\tau_{z_0}=0$，其中 $z_0=(0,0,\cdots,0)\in F_2^{(n-1)}$。

在 (3-4-20) 中，已给出剪接密钥 C_{n-1} 对 $G_n(2)$ 中极大圈 M_n 的作用。我们定义 C'_{n-1} 为 C_{n-1} 的相伴运算，其中

$$C'_{n-1}[(a(z,i),\ z,\ b(z,i))]=(a(z,i),\ z,\ b(z,i)+c_z),$$
$$i=1,\ 2;\ z\neq z_0\in F_2^{(n-1)},\qquad (3\text{-}4\text{-}26)$$

并记由 (3-4-26) 给定的全体弧为 $C'_{n-1}(M_n)$。

引理 4　由 $C'_{n-1}(M_n)$ 构造的图是非奇异的，且任何非含零环的全体非奇异函数均可由(3-4-26)产生。

证明　$C'_{n-1}(M_n)$ 的非奇异性由关系式

$$(a(z,1),\ b(z,1)+c_z)=(\bar{a}(z,2),\ \bar{b}(z,2)+c_z)$$
$$=(\bar{a}(z,2),\ \overline{b(z,2)+c_z})$$

即得。由 $c_z\in F_2,z\neq z_0\in F_2^{(n-1)}$ 的任意性，可知任何非含零环的非奇函异数均可由 (3-4-25) 产生。这时，只要将 (3-4-25) 代入 (3-4-4)，即可得到 τ_z 在 $z\neq z_0$ 处的任意变化，从而可以得到全部非含零环的非奇异函数，引理得证。

引理 5　若记 $\tilde{\tau}(n)$，$\tilde{\tau}'(n)$ 为由 M_n，$C'_{n-1}(M_n)$ 决定的组合表示，这时必有

$$\tau'_z=\tau_z+c_z,\quad z\in F_2^{(n-1)}\qquad (3\text{-}4\text{-}27)$$

成立。这里取 $c_{z_0}=0$。

定理 2　如 $\tilde{\tau}(n)$，$\tilde{\tau}'(n)$ 为 M_n，$C'_{n-1}(M_n)$ 的组合表示，$\tilde{\tau}(n+1)=\tilde{\tau}(n)^*$，$\tilde{\tau}'(n+1)=\tilde{\tau}'(n)^*$ 分别是它们的扩张，相应的元分别为 τ_s，τ'_s，其中 $s=(a_1,a_2,\cdots,a_n)\in F_2^{(n)}$，这时有关系式

$$\tau_s'=\begin{cases}\tau_s, & \text{若 } c_{s'}{}^{(s)}=c_{s''(s)},\\ \bar{\tau}_s, & \text{若 } c_{s'(s)}\neq c_{s''(s)},\end{cases}\qquad(3\text{-}4\text{-}28)$$

其中

$$z'(s)=(a_2,\cdots,a_n),\ z''=(a_1,\cdots,a_{n-1}).\qquad(3\text{-}4\text{-}29)$$

证明 从 τ_s 的定义 (3-4-8) 知，当 $\tilde{\tau}(n)$ 在 z 点发生接剪时 (即(3-4-26) 的 $c_z=1$ 时)，相应的 $\tilde{\tau}(n+1)$ 在 s 为 $(0,z)$，$(1,z)$．$(z,0)$，$(z,1)$ 四点的值发生了变化，即 $(0,z)$，$(1,z)$ 点的出弧及 $(z,0)$，$(z,1)$ 点的入弧发生了变化，因此 τ_s 的值发生了变化。这时必有：

若 $c_{s'(s)}=c_{s''(s)}$，则 s 点的出、入弧都不变或同时发生变化，且 τ_s 也不变。

若 $c_{s'(s)}\neq c_{s''(s)}$，则 s 点的出、入弧中必有一变化而另一弧不变，因此 τ_s 值变化，此即 (3-4-28) 成立，定理得证。

以下我们记 $(\tilde{\tau}(n),\ \bar{\tilde{\tau}}(n))$ 为两个互补的非奇异函数，$\bar{\tilde{\tau}}(n)$ 为非含零环的，则 $\tilde{\tau}(n)$ 为含零环的。又记 M_n 为 $G_n(2)$ 中的任一极大圈，这时必有剪接密钥 C_{n-1}，使 $\bar{\tilde{\tau}}(n)=C_{n-1}(M_n)$ 成立。若同时记 $\tilde{\tau}(n)$ 的圈为 Q_i，$i=0,1,\cdots,k$，其中 Q_0 为 $(0,0,\cdots,0)\to(0,0,\cdots,0)$ 环。这时我们得到一个对 $(M_n,\ \tilde{\tau}(n))$ 可作与 4.2 段中相同的定义，使 Q_i 在 M_n 中的首元为 S_i，且 S_i 在 M_n 中的次序就是 Q_i 的次序。这里同样取 M_n 的起点为 $S_0=(0,0,\cdots,0)$，而 S_i 的下标即为 S_i 在 M_n 中的次序。

定义 2 我们称 $S_0(M_n,\ \tilde{\tau}(n))$ 为 $(M_n,\ \tilde{\tau}(n))$ 的变动点，若 $S_0(M_n,\ \tilde{\tau}(n))$ 由 $S(H_n,\ \tilde{\tau}(n))$ 中无重复点构成，而 $S(\cdot,\cdot)$ 由以下点构成：

(i) 全体 Q_i 的首元 S_i，$i=0,1,\cdots,k$。

(ii) 是 C'_{n-1} 但非 C_{n-1} 剪接的端点，也就是全体

$$\{(a(z,2),z),(z,b(z,2)):c_z=1\}.\qquad(3\text{-}4\text{-}30)$$

定理 3 如 $(\tilde{\tau}(n),\ \bar{\tilde{\tau}}(n))$ 为互补对，$\bar{\tilde{\tau}}(n)=C'_{n-1}(M_n)$，$M_n$

为 $G_n(2)$ 的 M-序列，且 $\overrightarrow{\tau}(n)$ 的扩张为 $\tilde{\tau}(n+1)$，则由 $C_{n-1}(M_n)$ 产生的 M-序列的组合表示 $\tilde{\tau}'(n+1)$ 为

$$\tau'_i=\begin{cases}\tau_i, & \text{若 } S\notin S_0(M_n,\ \tilde{\tau}(n)),\\ \bar{\tau}_i, & \text{若 } S\in S_0(M_n,\ \tilde{\tau}(n)).\end{cases}\qquad(3\text{-}4\text{-}31)$$

证明　若 C_{n-1} 只有一个点的剪接，则 C'_{n-1} 将 M_n 分成两个圈，如图 3-2 所示，其中大圆为 M_n。因为 $(s,\ t)=(a(z,\ 1),\ z,\ b(z,\ 1))$，则 $(s^*,\ t')=(a(z,\ 2),\ z,\ b(z,\ 2))$。于是，$C_{n-1}$ 将 $(s,\ t)$ 弧变为 $(s,\ t')$，C'_{n-1} 将 $(s^*,\ t')$ 变为 $(s^*,\ t)$。$C_{n-1}(M_n)$ 为由 $s_0\to t\to t'\to s_0$，$t\to s^*\to t$ 的两个圈组成，这时，由 $C'_{n-1}(M_n)$ 产生的完备回路 W_n 的形成过程与本节定理 1 的过程相似，我们只要将 $(s,\ t)$ 弧与 $(s,\ t')$ 弧的编号次序更改即可。将完备回路与 $C'_{n-1}(M_n)$ 中的弧的走向比较，可见在 Q_t 的首元处及弧 $(s^*,\ t')$ 的两个端点处发生变化，这是因为 $C_{n-1}(M_n)$ 不改变 $(s^*,\ t')$，$(s^*,\ t)$ 弧的编号位置，而 $C'_{n-1}(M_n)$ 改变编号位置。

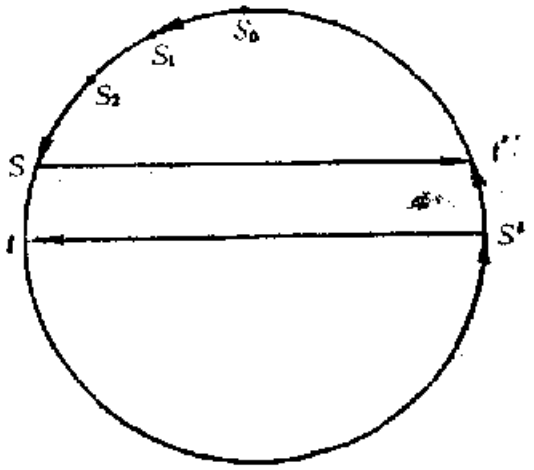


图 3-2　M_n，$C'_{n-1}(M_n)$ 关系图

对 C_{n-1} 有两个以上剪接点的情形，我们有过类似讨论，对此不再详述。

利用本节定理 2，的非奇异函数的性质直接构造 M-序列，有关步骤如下：

M_2-Ⅰ　由 M_n，C_{n-1} 写出互补的非奇异函数 $(\tilde{\tau}(n),\ \overrightarrow{\tau}(n))$，其中 $\overrightarrow{\tau}(n)$ 为 $C'_{n-1}(M_n)$ 的组合表示，由 (3-4-27) 给定。

M_2-Ⅱ　由 M_n 的扩张写出 $C'_{n-1}(M_n)$ 扩张的组合表示，即由 (3-4-28) 公式确定 $C'_n(M_n)$ 扩张的组合表示。

M_2-Ⅲ　写出 $\tilde{\tau}(n)$ 中的全体变动点，即 $\tilde{\tau}(n)$ 中圈的首元及

(3-4-30)的剪接弧，且由(2-4-31)确定所求完备回路的组合表示。

例3 我们任取一个例2中的完备回路M_4，及一个C_3的剪接算子，由上述非奇异函数性质构造$M_4(2)$-序列。

解 若取M_4为例2的$\tau_0(4)$，即取$\tilde{\tau}'(4)=(10101101)$为$M_4$的组合表示，而剪接算子为

$$C_3=(c_0,\cdots,c_7)=(00010100),$$

求相应的$M_5(2)$-序列。这时有

(1) 按关系式(3-4-27)可写出$C_3'(M_4)$的组合表示

$$\tilde{\tau}(4)=\tilde{\tau}'(4)+C_3=(10101011),$$

这时，

$$\tilde{\tau}(4)=(01010100).$$

(2) 因为

$$\begin{aligned}M_4=\{&0000\to0001\to0011\to0111\to1111\to1111\to1110\\&\to1100\to1000\to0111\to1011\to0110\to1101\to1010\\&\to0100\to1000\to0000\},\end{aligned}$$

因此M_4^*的组合表示为

$$\tilde{\tau}(5)=(\tau_0,\tau_1,\cdots,\tau_{15})=(0010010111101010).$$

这时，$C_3'(M_4)^*$的组合表示由(3-4-28)给定为

$$\tilde{\tau}'(5)=(\tau_0',\tau_1',\cdots,\tau_{15}')=(0011001011011010)$$

(3) $\tilde{\tau}(4)$的圈为：$0000\to0000$；$1111\to1111$及$0001\to0010\to0100\to1001\to0011\to0110\to1101\to1010\to0101\to1011\to0111\to1110\to1100\to1000\to0001$。

因此

$$\begin{aligned}S_0(M_4,C_3)&=\{(0000),(1111),(0001),(0110)(1010)\}\\&=\{0,15,8,6,5\}.\end{aligned}$$

这时得M_5的组合表示

$$\tau''(5)=(1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1).$$

即为所求。若由 $\tau''(5)$ 写出的M-序列为

$$M_5=\{00000\to00001\to00010\to00100\to01001\to10011$$
$$\to00110\to01100\to11001\to10010\to00101\to01010$$
$$\to10101\to01011\to10110\to01101\to11011\to10111$$
$$\to01110\to11100\to11000\to10001\to00011\to00111$$
$$\to01111\to11111\to11110\to11101\to11010\to11000$$
$$\to01000\to10000\to00000\},$$

则与所求结果一致。

本节中介绍的两种计算方法，对 $M_n(2)$-序列的寻找过程 有一定程度的简化。它可由 M_n,C_{n-1} 直接求出 M_{n+1} 的组合表示,且在 M_n 给定的条件下，由 C_{n-1} 的变化可同时找到一系 列 M_{n+1}-序列。在[5]、[6]、[15]、[19]、[20]等文中，对 M-序列的构造过程也有许多刻划与分析，对此不一一列举。

第 四 章

随机序列的平均非线性复杂度

§1 随机序列的 Markov 链与平均非线性复杂度

1.1 随机序列的平均非结性复杂度

正如第一章§1 所定义的那样,我们称

$$\bar{X}=(X_0, X_1, X_2, \cdots) \tag{4-1-1}$$

为完全的随机序列，若 $X_0, X_1, \cdots$是独立同分布的随机变量，且每个 X_i 在 F_2 上取均匀分布,这时对任何一组不同的 $i_1, \cdots, i_k$,

$$P_r\{(X_{i_1}, \cdots, X_{i_k})=(a_{i_1}, \cdots, a_{i_k})\}\overset{*}{=}\frac{1}{2^k}. \tag{4-1-1a}$$

同样我们记

$$X^{(p)}=(X_1, X_2, \cdots, X_{p-1}) \tag{4-1-2}$$

为随机向量,它的样本值为

$$a^{(p)}=(a_0, a_1, \cdots, a_{p-1}), a_i\in F_2. \tag{4-1-3}$$

显然,对任何 $a^{(p)}\in F_2^{(p)}$, 有

$$P_r\{X^{(p)}=a^{(p)}\}\overset{*}{=}\frac{1}{2^p}.$$

对于任何(4-1-3)中向量 $a^{(p)}$, 在第一章§1中我们已定义其非

线性复杂度为

$$C_N(a^{(p)}) \triangleq \min\{n: \text{存在 } f(x^{(n)}) \text{生成 } a^{(p)}\}。$$

当 $X^{(p)}$ 取不同的 $a^{(p)}$ 时，我们得到不同的非线性复杂度，记 $C_N(X^{(p)})$为随机向量的非线性复杂度函数，简称随机非线性复杂度。这是一个随机变量，且称

$$p(p, k) \triangleq P_r\{C_N(X^{(p)}) = k\} \tag{4-1-4}$$

为 $C_N(X^{(p)})$的分布函数，它表示 $C_N(X^{(p)})$为 k 的概率，这时

$$E\{C_N(X^{(p)})\} \triangleq \sum_{k=0}^{p} k \cdot p(p, k) \tag{4-1-5}$$

为 $C_N(X^{(p)})$的平均非线性复杂度。在(4-1-5)中，求和的上、下界是由关系式

$$0 \leqslant C_N(a^{(p)}) \leqslant p$$

对任何 $a^{(p)} \in F_2^{(p)}$而得。

在本章中，我们讨论 $p(p, k)$取值的情况及对 $E\{C_N(X^{(p)})\}$的估计，由此可以知道关于非线性复杂度的有关特性。

1.2　随机序列状态转移的 Markov 链

对(4-1-1)的随机序列 $\tilde{X}$，我们称

$$\begin{aligned} S_i(k) &= X(i-k, i-1) \\ &= (X_{i-k}, X_{i-k+1}, \cdots, X_{i-1}) \end{aligned} \tag{4-1-6}$$

为 $\tilde{X}$ 在时刻 i 处的 k 维状态，相应的样本值为

$$S_i(k) = a(i-k, i-1) = (a_{i-k}, \cdots, a_{i-1})。 \tag{4-1-6a}$$

若 k 固定，则序列

$$\tilde{S}(k) = (S_k(k), S_{k+1}(k), \cdots) \tag{4-1-7}$$

为一个新的随机序列，这时 $S_i(k)$, $i = k, k+1, \cdots$ 为在 $F_2^{(k)}$上取值的随机变量，它们具有以下特性：

(1) 每个 $S_i(k)(i = k, k+1, \cdots)$在 $F_2^{(k)}$上取均匀分布，也就是对任何 $a^{(k)} \in F_2^{(k)}$，总有

$$P_r\{S_i(k)=a^{(k)}\}=\frac{1}{2^k}。\qquad(4\text{-}1\text{-}8)$$

成立，这个关系式由(4-1-1a) 即得。

(2) 无后效性，即当 $S_{i+1}(k)$固定时 $S_i(k)$ 与 $S_{i+2}(k)$ 相互独立。

关于性质(2)的证明，由 $S_i(k)$的定义即得，因为(4-1-6)中若 $S_{i+1}(k)$固定，则有

$$(X_{i-k+1}, X_{i-k+2}, \cdots, X_i)=(a_1, \cdots, a_k)。\qquad(4\text{-}1\text{-}9)$$

成立，这时

$$S_i(k)=(X_{i-k}, a_1, \cdots, a_{k-1}),$$
$$S_{i+2}(k)=(a_2, \cdots, a_k, X_{i+1}),$$

因为 X_{i-k} 与 X_{i+1} 是相互独立的，所以 $S_i(k)$ 与 $S_{i+2}(k)$ 在 $S_{i+1}(k)$固定条件下相互独立，因此关于 $\tilde{S}(k)$的无后效性成立。

由随机序列的定义知道，一个具有无后效性的随机序列为一个 Markov 链，因此 $\tilde{S}(k)$是一个 Markov 链。由随机过程理论知，一个 Markov 链的分布情形是由其初始分布与转移概率矩阵决定，当 $i=k$ 时，(4-1-8)就是 $S_i(k)$的初始分布，所以我们只要讨$S_i(k)$论的转移概率矩阵即可。对任何

$$a^{(k)}=(a_1, \cdots, a_k),\ b^{(k)}\triangleq(b_1, \cdots, b_k)\in F_2^{(k)},$$

我们称

$$P_i(a^{(k)}/b^{(k)})\triangleq P_r\{S_{i+1}(k)=a^{(k)}/S_i(k)=b^{(k)}\},\qquad(4\text{-}1\text{-}10)$$

为 $S_i(k)=a^{(k)}$ 时向 $S_{i+1}(k)=b^{(k)}$转移的概率，(4-1-10)式的右边为条件概率。

当 $a^{(k)}, b^{(k)}\in F_2^{(k)}$变化时，由(4-1-10)我们可得到一个 $2^k\times 2^k$ 阶矩阵，这就是 $\tilde{S}(k)$在时刻 i 处的状态转移概率矩阵，记为

$$P_i=[p_i(a^{(k)}/b^{(k)})]_{2^n\times 2^n}。\qquad(4\text{-}1\text{-}11)$$

若对 $F_2^{(k)}$中的元进行编号，即记

$$j = j(a^{(k)}) \overset{*}{=} a_1 + 2 \cdot a_2 + \cdots + 2^{k-1} \cdot a_k, \qquad (4\text{-}1\text{-}12)$$

则 $F_2^{(k)}$ 可表示为集合

$$F_2^{(k)} = \{0, 1, \cdots, 2^k - 1\}. \qquad (4\text{-}1\text{-}12a)$$

这时，(4-1-11)的转移概率矩阵可表示为

$$P_i = [p_i(j/j')]_{2^n \times 2^n}, \qquad (4\text{-}1\text{-}11a)$$

其中 $j = j(a^{(k)})$，$j' = j(b^{(k)})$。

在第一章 §5 中，我们已给出 $G_n(2)$图的联系矩阵

$$B[G_n(2)] = [d_{j,j'}]_{2^n \times 2^n}, \qquad (4\text{-}1\text{-}13)$$

其中

$$d_{j,j'} = \begin{cases} 1, \text{若}(j', j) \in L_n, \\ 0, \text{否则}, \end{cases} \qquad (4\text{-}1\text{-}13a)$$

L_n 为 $G_n(2)$ 中全体弧，这时 $B[G_n(2)]$矩阵可表示为

$$B(G_n(2)] = \begin{bmatrix} I_n \\ I_n \end{bmatrix},$$

$$I_n = \left[\begin{array}{ccccc} 1\ 1 & & & & 0 \\ & 1\ 1 & & & \\ & & 1\ 1 & & \\ & & & \ddots & \\ 0 & & & & 1\ 1 \end{array}\right] \Big\} 2^{n-1} \qquad (4\text{-}1\text{-}13b)$$

的形式

定理 1　$\tilde{S}(k)$是一个齐次的 Markov 链，即它的转移概率矩阵 P_i 与 i 无关，且满足

$$P_i \overset{*}{=} \frac{1}{2} \cdot B[G_k(2)]', \qquad (4\text{-}1\text{-}14)$$

其中 $B[\cdot]'$ 为 $B[\cdot]$矩阵的转置，P_i 由(4-1-11)定义。

证明　因为 $S_i(k) = a_0^{(k)} = (a_1^0, a_2^0, \cdots, a_k^0)$ 的下一步 $S_{i+1}(k)$ 的可能状态为

$$(a_2^0, a_3^0, \cdots, a_k^0, a_{k+1}),\ a_{k+1}=0 \text{ 或 } 1。$$

且

$$P_r\{S_{i+1}(k)=(a_2^0, \cdots, a_k^0, a_{k+1})/S_i(k)=(a_1^0, \cdots, a_k^0)\}$$

$$=P_r\{X_i=a_{k+1}\}\overset{*}{=}\frac{1}{2}。$$

另一方面，若记

$$j=j(a_0^{(k)})\overset{*}{=}a_1^0+2\cdot a_2^0+\cdots+2^{k-1}\cdot a_k^0,$$

则

$$j'=j(a_2^0, \cdots, a_k^0, a_{k+1})\overset{*}{=}L\frac{j}{2}J+a_{k+1}\cdot 2^{k-1}$$

$$\overset{*}{=}L\frac{j}{2}\ j \text{ 或 } L\frac{j}{2}\ j+2^{k-1}, \tag{4-1-15}$$

这时 P_i 矩阵的元为

$$P_i(j'/j)\overset{*}{=}\begin{cases}\frac{1}{2}, & \text{若(4-1-15)成立,}\\ 0, & \text{否则,}\end{cases} \tag{4-1-16}$$

此即(4-1-14)成立。定理得证。

1.3 关于状态的 r-步转移概率矩阵

所谓状态的 r-步转移概率矩阵，就是从随机状态 $S_i(k)$ 到 $S_{i+r}(k)$ 的转移概率矩阵，因此(4-1-11)阵是一个 1-步转移概率矩阵。记

$$P^{(r)}=[P^{(r)}(j'/j)]_{2^k\times 2^k} \tag{4-1-17}$$

为 $\tilde{S}(k)$ 的 r-步转移概率矩阵。由 $\tilde{S}(k)$ 的齐次性知，$P^{(r)}$ 与出发状态 i 无关，这里

$$P^{(r)}(j'/j)=P_r\{S_{k+r}(k)=j'/S_k(k)=j\}。\ (4\text{-}1\text{-}17a)$$

现在计算(4-1-17)式，由条件概率与 Markov 的无后效性可得

$$p^{(2)}(j'/j)\overset{*}{=}\sum_{j''=0}^{2^k-1}P_r\{S_{k+1}(k)=j''/S_k(k)=j\}\cdot$$

$$P_r\{S_{k+2}(k)=j'/S_k(k)=j,\ S_{k+1}(k)=j''\}$$

$$\stackrel{*}{=}\sum_{j''=0}^{2^k-1}P(j''/j)\cdot P(j'/j''), \qquad (4\text{-}1\text{-}18)$$

其中 $P(j'/j)$为(4-1-11a) 的转移概率矩阵。因此,由矩阵的运算定义有

$$P^{(2)}\stackrel{*}{=}P^2\stackrel{*}{=}\frac{1}{4}\{B[G_k(2)]'\}^2 \qquad (4\text{-}1\text{-}18a)$$

成立,其中 $P^{(2)}$ 为(4-1-11a) 的 1-步转移概率矩阵,P^2 为 P 的 2 次幂。

定理 2　Markov 链 $\tilde{S}(k)$的 r- 步转移概率矩阵为

$$P^{(r)}=P^r\stackrel{*}{=}\frac{1}{2^r}\{B[G_k(2)]^r\}'。 \qquad (4\text{-}1\text{-}19)$$

证明　这个推导过程与 $r=2$ 的情形相同,我们只要多次应用条件概率与 Markov 链的无后效性即得。对于(4-1-19)的第二个等式,只要利用矩阵运算性质

$$(B')^r=(B^r)'$$

即得,由此定理得证。

为了给出 $P^{(r)}$ 的确切表达式,只要利用(4-1-19)给出 $B[G_k(2)]^r$ 即可。由矩阵运算可得如下结论:

(1) 当 $r<k$ 时,有

$$B[G_k(2)]^r=\left.\begin{bmatrix} I_k(r)\\ I_k(r)\\ \cdots\\ I_k(r)\end{bmatrix}\right\}2^r \qquad (4\text{-}1\text{-}20)$$

成立,其中

$$I_k(r)=\left.\begin{bmatrix} \overbrace{1\ 1\cdots 1}^{2^r\text{个}} & & & 0\\ & 1\ 1\cdots 1 & & \\ & & \ddots & \\ 0 & & & 1\ 1\cdots 1\end{bmatrix}\right\}2^{k-r}。 \qquad (4\text{-}1\text{-}20a)$$

(2) 当 $r \geqslant k$ 时，

$$B[G_k(2)]^r \overset{*}{=} 2^{r-k}\left\{\overbrace{\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ & & \cdots\cdots & & \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}}^{2^k\text{列}}\right\}2^k\text{行} \qquad (4\text{-}1\text{-}21)$$

关于(4-1-20)与(4-1-21)的证明，只要对 $B[G_k(2)]$逐次进行幂运算即得，对此不再详述。

§2 随机序列的平均复杂度估计

2.1 平均复杂度的估计问题

现在考虑随机序列 $\tilde{X}=(X_0, X_1, \cdots)$的非线性复杂度的均值估计问题。在本章§1中，我们已对 $X^{(p)}=(X_0, X_1, \cdots, X_{p-1})$ 的平均非线性复杂度作了定义，即为

$$E\{C_N(X^{(p)})\} \overset{*}{=} \frac{1}{2^p}\sum_{a^{(p)}\in V_2^{(p}} C_N(a^{(p)})$$

$$\overset{*}{=}\sum_{k=0}^{p} k\cdot p(p,k), \qquad (4\text{-}2\text{-}1)$$

其中 $p(p,k)$为(4-1-4)定义。下面对这个 $E\{C_N(X^{(p)})\}$ 的值进行估计。

首先在线性情形，许多论文对线性复杂度的均值问题进行了讨论，且得到

$$E\{C_L(X^{(p)})\} \overset{*}{=} o(p) \qquad (4\text{-}2\text{-}2)$$

的一系列估计，其中 $C_L(a^{(p)})$为 $a^{(p)}$的线性复杂度。我们认为，非线性的情形与线性情形有极大的区别，得到的结果是

$$E\{C_N(X^{(p)})\}\overset{*}{=}O(\log p). \tag{4-2-3}$$

在(4-2-2)与(4-2-3)中，$o(p)$ 与 $O(\log p)$ 分别为 p 的等价无穷大量与 $\log p$ 的同阶无穷大量，也就是

$$\lim_{p\to\infty}\frac{1}{p}E\{C_L(X^{(p)})\}=1$$

与存在常数 $0<\gamma_0<\gamma_1<\infty$，使

$$\gamma_0\overset{*}{\leqslant}\underline{\lim_{p\to\infty}}\frac{1}{\log p}E\{C_N(X^{(p)})\}$$

$$\overset{*}{\leqslant}\overline{\lim_{p\to\infty}}\frac{1}{\log p}E\{C_N(X^{(p)})\}\leqslant\gamma_1 \tag{4-2-4}$$

成立。为此我们作以下讨论。

为了简单起见，先讨论随机序列的非奇异复杂度 $C_S(X^{(p)})$，因为在第三章 §1 中我们已证明对任何 $a^{(p)}\in F_2^{(p)}$，总有

$$C_N(a^{(p)})\leqslant C_S(a^{(p)})\leqslant C_N(a^{(p)})+1$$

成立，因此对随机序列同样有

$$C_N(X^{(p)})\leqslant C_S(X^{(p)})\leqslant C_N(X^{(p)})+1 \tag{4-2-5}$$

成立，为此我们只要估计 $C_S(X^{(p)})$ 即可。

2.2　关于 $\tilde{S}(k)$ 序列的若干性质

对随机序列 $\tilde{S}(k)$，在本章 §1 中我们已给出了它的转移概率矩阵，由此即得

引理　对随机序列 $\tilde{X}$ 的状态 Markov 链 $\tilde{S}(k)$ 的任何状态 $k\leqslant i<j<$，总有

$$P_r\{S_i(k)=S_j(k)\}\overset{*}{=}2^{-k} \tag{4-2-6}$$

成立。

证明　记 $r=j-i$，则 $r\geqslant 1$，且由上节定理 2 知

$$P_r\{S_i(k)=S_j(k)\}\overset{*}{=}\sum_{t\in F_2^{(k)}}P_r\{S_i(k)=S_j(k)=t\}$$

$$\overset{*}{=}\sum_{t\in F_2^{(k)}}p(t)P^{(r)}(t/t),$$

其中 $P^{(r)}(t/t)$为 $\tilde{S}(k)$的r步转移概率矩阵，而

$$p(t)=P_r\{S_i(k)=t\}\overset{*}{=}2^{-k}.$$

由关系式(4-1-20)、(4-1-21)知、当 $r<k$ 时，矩阵 $B[G_k(2)]^r$ 中有 2^r 个对角线上的点为 1，其余为 0。又由关系式(4-1-19)知

$$\sum_{t\in F_2^{(k)}}^{1*} p^{(r)}(t/t)=1,$$

因此关系式(4-2-6)成立。

对 $r\geqslant k$ 情形，由关系式(4-1-19)、(4-1-21)有

$$\sum_{t\in F_2^{(k)}}^{*} p^{(r)}(t/t)\overset{*}{=}\frac{1}{2^r}\sum_{t\in F_2^{(k)}} 2^{r-k}=1$$

成立，由此得(4-2-6)成立。引理得证。

2.3 关于平均非线性复杂度的估计公式

定理 1 对随机序列 $\tilde{X}$ 的平均非线性复杂度 $E\{C_N(X^{(p)})\}$，存在两个常数 θ_0 与 θ_1，使

$$E\{C_N(X^{(p)})\}\overset{*}{\leqslant}\theta_0 k_0+\theta_1. \tag{4-2-7}$$

成立，其中 $k_0=\lfloor\log p\rfloor$。

证明 取 $k_1=2k_0+1$，这时显然有 $p^2\leqslant 2^{k_1+1}$，由 $E\{C_N(X^{(p)})\}$ 的定义有

$$E\{C_N(X^{(p)})\}\overset{*}{=}\sum_{k=0}^{p}k\cdot P_r\{C_N(X^{(p)})=k\}$$

$$\overset{*}{\leqslant}k_1+\sum_{k=k_1+1}^{p}k\cdot P_r\{C_N(X^{(p)})\geqslant k\} \tag{4-2-8}$$

成立。我们估计(4-2-8)不等式右边的值，因为 $C_N(X^{(p)})\leqslant C_S(X^{(p)})$，所以

$$P_r\{C_N(X^{(p)})\geqslant k\}\leqslant P_r\{C_S(X^{(p)})\geqslant k\}$$

$$=P_r\{\text{有一对 } k\leqslant i<i'<p,\text{使 } S_i(k)=S^{ii'}_i(k)\text{成立}\}$$

$$\overset{*}{\leqslant}\frac{(p-k)(p-k-1)}{2}\cdot 2^{-k}\overset{*}{=}(p-k)(p-k-1)2^{-(k+1)}$$

成立，其中系数$\frac{1}{2}(p-k)(p-k-1)$为由$k\leqslant i<i'<p$的取法而定，因此

$$E\{C_N(X^{(p)})\}\overset{*}{\leqslant}k_1+\sum_{k=k_1+1}^{p}k(p-k)(p-k-1)2^{-(k+1)}$$

$$\overset{*}{\leqslant}k_1+(k_1+3)\frac{p^2}{4}\cdot 2^{-(k_1+1)}\overset{*}{\leqslant}\frac{5}{4}k_1+\frac{3}{4},\quad(4\text{-}2\text{-}9)$$

其中，第二个不等式由$k(p-k)\overset{*}{\leqslant}\frac{p^2}{4}$及其他幂级数性质而得；第三个不等式由$p^2\overset{*}{\leqslant}2^{-(k_1+1)}$而得。将$k_1\overset{*}{=}2k_0+1$代入(4-2-9)得

$$E\{C_N(X^{(p)})\}\overset{*}{\leqslant}\frac{5}{2}k_0+2,\qquad(4\text{-}2\text{-}10)$$

这时$(\theta_0,\theta_1)=\left(\frac{5}{2},2\right)$为定理所证。

由(4-2-10)我们得到$E\{C_N(X^{(p)})\}$的上界的估计，若进一步应用 Markov 的链的性质，对(4-2-9)的不等式还可有更精确的估计，对此不再详述。

定理 2　对平均非线性复杂度$E\{C_N(X^{(p)})\}$，同样有下界估计式

$$E\{C_N(X^{(p)})\}\overset{*}{\geqslant}\theta_2k_0-\theta_3,\qquad(4\text{-}2\text{-}11)$$

其中$k_0=\lfloor\log p\rfloor$，θ_2,θ_3为两非负常数。

证明　由移位寄存器的性质知，如$C_N(Q^{(p)})=k$，则$a^{(p)}$的周期不大于2^k。以下我们定义

$$D_0(p_0,p)=\{a^{(p)}\in F_2^{(p)};\ a^{(p)}\text{的周期为}\ p_0\},\quad(4\text{-}2\text{-}12)$$

若$p\leqslant p_0$，则必有$a^{(p)}\in D(p_0,p)$，因此必有

$$\|D_0(p_0,p)\|\overset{*}{=}2^p$$

成立。我们考虑$p>p_0$的情形，这时

$$\|D_0(p_0,p)\|\overset{*}{\leqslant}2^{p_0}$$

成立，如果记

$$D_1(k,p)=\bigcup_{p_0=1}^{2^k}D_0(p_0,p),$$

$$D_2(k,p)=\{a^{(p)}: C_N(a^{(p)})\leqslant k\}, \qquad (4\text{-}2\text{-}13)$$

则必有

$$D_2(k,p)\supset D_1(k,p),$$

且

$$\|D_1(k,p)\|\overset{*}{\leqslant}\sum_{p_0=1}^{2^k}2^{p_0}\overset{*}{=}2(2^{2k}-1), \qquad (4\text{-}2\text{-}14)$$

因此(4-2-14)不等式对 $D_2(k,p)$也成立. 由(4-2-1)得

$$E\{C_N(X^{(p)})\}\overset{*}{\geqslant}\sum_{k=k_0-1}^{p}k\cdot P_r\{C_N(X^{(p)})=k)\}$$

$$\overset{*}{\geqslant}(k_0-1)P_r\{C_N(X^{(p)})\geqslant k_0-1\}$$

$$\overset{*}{=}(k_0-1)[1-P_r\{C_N(X^{(p)})<k_0-1\}]$$

成立; 由(4-2-14)知

$$P_r\{C_N(X^{(p)})<k_0-1\}\overset{*}{\leqslant}\exp_2[-(p-2^{k_0-1}+2)]$$

$$\overset{*}{\leqslant}\exp_2(-2^{k_0-1}-2)$$

成立. 因此当 $p\geqslant 4$ 时, $k_0\geqslant 2$,且有

$$E\{C_N(X^{(p)})\}\overset{*}{\geqslant}(k_0-1)[1-\exp_2(-2^{k_0-1}-2)]. \qquad (4\text{-}2\text{-}15)$$

若记(4-2-15)不等式右边中括号里的值为

$$\theta(p)\overset{*}{=}1-\exp_2(-2^{k_0-1}-2)],$$

则当 $p\geqslant 4, k_0\geqslant 2$ 时, $\theta(p)\overset{*}{\geqslant}1-2^{-4}$; 当 $p\to\infty$ 时, $\theta(p)\to 1$. 这时我们取

$$\theta_2=\theta_3=\theta(4)\overset{*}{=}\frac{15}{16},$$

即为定理所求, 这时不等式(4-2-11) 对任何 $p\geqslant 4$ 成立, 定理得证.

事实上, 在定理 2 的证明中我们得到更多的结论, 也就是有关系式

$$E\{C_N(X^{(p)})\}\overset{*}{\geqslant}(k_0-1)\left[-\exp_2\left(-\frac{p}{2}-2\right)\right] \quad (4\text{-}2\text{-}16)$$

成立. 这时(4-2-16)的下界是一个与 $\log p$ 等价的无穷大量.

例　求 $X^{(5)}$ 的平均非线性复杂度.

解　对 $F_2^{(5)}$ 中向量的非线性复杂度列表如下:

表 3-1　$a^{(5)}$ 的非线性复杂度

$a^{(5)}$	$C_N(a^{(5)})$	$a^{(5)}$	$C_N(a^{(5)})$
00000	0	01001	2
00001	4	10001	3
00010	3	00110	2
00100	2	01010	1
01000	2	10010	2
10000	1	01100	2
00011	3	10100	3
00101	2	11000	2

由对称性，另外 16 个向量(即表 3-1 中 16 个向量的补向量 $\bar{a}^{(5)}$)的复杂度由关系式 $C_N(a^{(p)})=C_N(\bar{a}^{(p)})$ 即得，因此平均非线性复杂度为

$$E\{C_N(X^{(5)})\}\overset{*}{=}\frac{1}{2^5}\left((1\times 4+2\times 16+3\times 8+4\times 2)\right.$$
$$=2.125,$$

显然在本节定理 1，2 的上、下界之内.

第 五 章

复合前馈序列的若干问题

§1 复合前馈网络与它的序列

1.1 复合前馈序列的一般定义与问题

近几年来，人们对复合前馈网络加密体制予以更多的关注。所谓复合前馈序列，就是由若干序列(移位寄存器序列或随机序列)通过一定的方式合成为一个序列，这个合成序列就称为复合前馈序列或复合序列。以下记

$$\bar{a}_i=(a_{i1}, a_{i2}, a_{i3}, \cdots), a_{ij}\in F_q,$$
$$i=1, 2, \cdots, n, \qquad (5\text{-}1\text{-}1)$$

为一组 q 值的周期序列，它可以是移位寄存器序列，也可以是周期随机序列的样本值，我们称之为前馈网络中的子序列，设

$$z=f(x_1, x_2, \cdots, x_n) \qquad (5\text{-}1\text{-}2)$$

为一个 $F_q^{(n)}\to F_q$ 的非线性组合函数，若把这个 $f(x^{(n)})$ 看作 $\bar{a}_i$ 的合成函数，则由 $f(x^{(n)})$ 可产生序列

$$c_j=f(a_{1j}, a_{2j}, \cdots, a_{nj}),$$
$$j=0, 1, 2, \cdots, \qquad (5\text{-}1\text{-}3)$$

它们的合成如图 5-1 所示。我们称

$$\bar{c}=(c_0, c_1, c_2, \cdots), c_i\in F_q, \qquad (5\text{-}1\text{-}4)$$

为 $\{\tilde{a}_1, \cdots, \tilde{a}_n\}$的复合序列，而称 $f(x^{(n)})$为生成函数或一个前馈网络的生成函数。

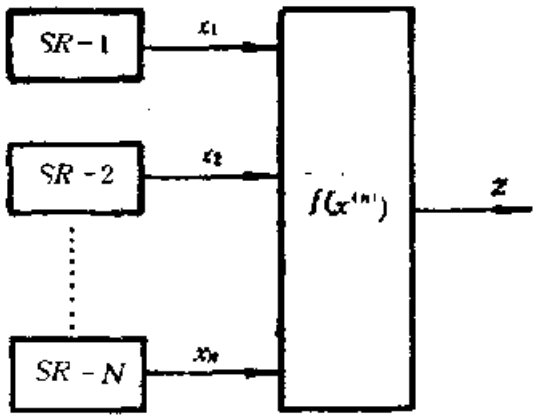


图 5-1　一般复合前馈网络与复合序列生成图

关于复合序列研究中，人们关心的问题大体上可分为两大类，即它们的统计特性与复杂性关系问题。所谓统计特性，即复合序列本身及复合序列与各子序列的统计性质，如相关性、分布类型、熵函数等，其中核心问题是相关免疫性，我们将在后面两节中作详细研究。

所谓复杂性，即讨论复合序列与子序列之间的复杂度的相互计算关系，目前许多文献注意力仍在线性复杂度上，且合成序列也比较特殊，在本书中我们不作详细讨论。

1.2　关于钟控复合序列

在合成序列中，不同的子序列可以起不同的作用，最典型的情形为“钟控”序列的情形，记

$$\tilde{a} = (a_0, a_1, \cdots), \tilde{b} = (b_0, b_1, \cdots)$$

为两个 q 值序列，若定义

$$b(i) = b(b_0, b_1, \cdots, b_i) \tag{5-1-5}$$

为$(b_0, b_1, \cdots, b_i)$的函数，且

$$c_i = a_{b(i)}, i = 0, 1, 2, \cdots, \tag{5-1-6}$$

这时称 $\tilde{c}$ 为由 $\tilde{a}, \tilde{b}$ 产生的钟控复合序列，其中 $\tilde{b}$ 序列决定合成序

列的时间位置，称为主选序列；而 $\tilde{a}$ 决定合成序列的数据来源，称为被选序列。

关于钟控序列的模型很多，以上只是最简单情形。一般可由几组主选序列与被选序列的复合，例如四个序列 $\tilde{a}$，$\tilde{b}$，$\tilde{c}$，$\tilde{d}$ 中有钟控的复合为

$$c_i = f(a_{b(i)}, c_{d(i)}), i = 0, 1, 2, \cdots, \quad (5\text{-}1\text{-}7)$$

其中 $f(x_1, x_2)$为一个二元非线性组合函数，$b(i)$，$d(i)$为(5-1-5)的函数，由 $\tilde{b}$，$\tilde{d}$ 产生，这时 c 序列为两组具有主选、被选序列的复合。另外，关于(5-1-5)的函数也可由多种定义形式，有如在 $q = 2$ 时 Jennings 序列取

$$b(i) \overset{*}{=} i + r(b_{i-h} + 2b_{i-h+1} + \cdots + 2^{h-1}b_i),$$

其中 h 是适当常数 $r(\cdot)$

$$\{0, 1, \cdots, 2^h - 1\} \to \{0, 1, \cdots, n-1\}$$

的函数，$n \geqslant 2^h$。

§2 相关免疫函数的判别与性质

2.1 相关免疫函数与熵漏的定义

在同步前馈网络中，有二个重要的特性，即相关免疫性与熵漏。它们反映了复合序列与子序列相关性中的一个重要特征。现在就其一般随机情形进行分析讨论。

设 $f(x_1, \cdots, x_n)$为一个 q 值 n 元的非线性组合函数，它表示前馈网络的输入为 F_q 上的元 x_1，x_2，$\cdots$，x_n 时，输出为

$$z = f(x_1, x_2, \cdots, x_n),$$

如图 5-2 所示，这时若 $f(\cdot)$ 的输入为随机变量

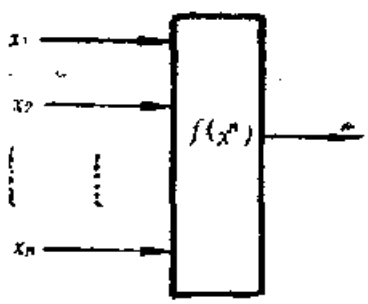


图 5-2 一般同步前网络运算函数

$$X_1, X_2, \cdots, X_n, \tag{5-2-1}$$

则 $f(\cdot)$的输出也为随机变量

$$Z = f(X_1, X_2, \cdots, X_n). \tag{5-2-2}$$

在本章中我们假定(5-2-1)的随机变量 $X_1, \cdots, X_n$ 为独立同分布，且每个 X_i 在 F_q 上取均匀分布，这时 z 的分布性质由 $f(x_1, \cdots, x_n)$函数决定。同样记

$$\alpha = \{i_1, i_2, \cdots, i_m\} \subset N = \{1, 2, \cdots, n\},$$

其中 $1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n$，这时

$$x(\alpha) = (x_i, i \in \alpha) = (x_{i_1}, \cdots, x_{i_m})$$

为 $x^{(n)} = (x_1, \cdots, x_n)$的部分向量，

$$x^{(n)} = (x(\alpha), x(\alpha^c)), \alpha^c = N - \alpha,$$

若记 $N_i = N - \{i\}$，这时

$$x^{(n)} = (x_i, x(N_i)).$$

定义 1　称 $f(x_1, \cdots, x_n)$ 为 m 阶相关免疫函数，若对任何 $\alpha \subset N$，$\|\alpha\| = m$，随机变量 $Z = f(X^{(n)})$ 总与 $X(\alpha)$相互独立，否则为非 m 阶相关免疫的。这里

$$X(\alpha) = (X_i, i \in \alpha) = (X_{i_1}, X_{i_2}, \cdots, X_{i_m})$$

为 $X^{(n)} = (X_1, \cdots, X_n)$的部分随机向量。

记

$$p_z(z) = P_r\{Z = z\},\ p_X(x(\alpha)) = P_r\{X(\alpha) = x(\alpha)\},$$

$$p(x(\alpha), z) = P_r\{X(\alpha) = x(\alpha), Z = z\} \tag{5-2-3}$$

为 $(X^{(n)}, z)$ 的联合概率分布与相应的边际分布，则 $f(x^{(n)})$ 为 m 阶相关免疫的充要条件为对任何 $x(\alpha) \in F_q^m$，$z \in F_q$，总有

$$p(x(\alpha), z) \overset{*}{=} p_X(x(\alpha)) \cdot p_z(z) \tag{5-2-4}$$

成立，或对任何 $\alpha \subset N$，$\|\alpha\| = m$，

$$I(Z; X(\alpha)) = 0 \tag{5-2-4a}$$

成立，其中 $I(Z; X(\alpha))$为随机变量 Z 与 $X(\alpha)$的交互信息，即

$$I(Z;X(\alpha))\overset{*}{=}\sum_{x(\alpha)\in F_q^{(m)}}\sum_{z\in F_q}p(x(\alpha),z)\log\frac{p(x(\alpha),z)}{p_X(x(\alpha))p_z(z)} \tag{5-2-5}$$

定义 2 对(5-2-2)的随机变量 Z,我们称

$$\varepsilon_0(f)\overset{*}{=}=\log q-H(Z) \tag{5-2-6}$$

为 $f(\cdot)$的熵漏,其中

$$H(Z)\overset{*}{=}-\sum_{z\in F_q}p_z(z)\log p_z(z) \tag{5-2-6a}$$

为 Z 的 Shannon 熵,称

$$\varepsilon_m(f)\overset{*}{=}\operatorname*{Max}_{\substack{\alpha:\alpha\subset N\\ \|\alpha\|=m}}[\log q-H(Z/X(\alpha))] \tag{5-2-7}$$

为 $f(\cdot)$的 m 阶熵漏,其中

$$H(Z/X(\alpha))\overset{*}{=}H(Z)-I(Z;X(\alpha)) \tag{5-2-7a}$$

为 Z 关于 $X(\alpha)$的条件熵。

相关免疫性与熵漏的概念均反映了前馈网络中各种数据之间的统计特性,如 $f(\cdot)$不具有相关免疫性,或熵漏存在,则人们可从输出数据 Z 中获得输入数据的各种信息,这在设计密码体制中应加以避免。

从相关免疫性的定义可见,以下性质是显然的。

引理 1 (i) 若 $f(x^{(n)})\equiv$常数,则 $f(\cdot)$为 n阶相关免疫的,对其他情形,$f(\cdot)$不可能是 n 阶相关免疫的。

(ii) 若 $f(\cdot)$ 为 m 阶相关免疫的,则 $f(\cdot)$ 必为 $m-1$ 阶相关免疫的。

(iii) 若 $f(\cdot)$为 m 阶相关免疫的,τ 为 N 上的置换函数,则

$$f_\tau(x_1,\cdots,x_n)\overset{\triangle}{=}f(x_{\tau(1)},\cdots,x_{\tau(n)}) \tag{5-2-8}$$

必为 m-阶相关免疫的。

(iv) 若 $f(\cdot)$为 m 阶相关免疫的,$g(\cdot)$ 为任何 $F_q\to F_q$ 的函数,则 $g[f(x_1,\cdots,x_n)]$ 也必为 m 阶相关免疫的。

证明略.

以下我们不讨论 $f(x^n)\equiv$常数情形，因此 $f(\cdot)$ 不可能是 n 阶相关免疫的. 同时称 $n-1$ 阶相关免疫的 $f(\cdot)$ 为相关免疫函数.

2.2　相关免疫性的判别条件

下面先给出一个 q 值 n 元 m 阶相关免疫函数的一个等价判别条件，对任何(5-2-2)的 $f(x_1,\cdots,x_n)$，记

$$f^{-1}(z/a(\alpha))=\{x(\alpha^c):f(a(\alpha),x(\alpha^c))=z\},\quad (5\text{-}2\text{-}8)$$

即 $f(\cdot)$在 $x(\alpha)=a(\alpha)$条件下的逆像，其中 $a(\alpha)=(a_i,\ i\in\alpha)$ 与 $x(\alpha)$定义相同. 因为在第一章中我们已定义过 $f(x^n)$的组合表示为

$$A_z[f(x^n)]=\{x^n:f(x^{(n)})=z\},\ z\in F_q,\quad (5\text{-}2\text{-}9)$$

这时有

$$f^{-1}(z/a(\alpha))=A_z[f(x^{(n)})][a(\alpha)],\quad (5\text{-}2\text{-}8a)$$

其中集合 $A[a(\alpha)]$表示 A 在 $a(\alpha)$上的切口，即

$$A[a(\alpha)]=\{x(\alpha^c):(a(\alpha),x(\alpha^c))\in A\}.\quad (5\text{-}2\text{-}10)$$

以下记

$$\tilde{\alpha}_m=\{\alpha:\alpha\subset N,\ \|\alpha\|=m\}.\quad (5\text{-}2\text{-}11)$$

定义 3　称 $f(x^{(n)})$ 为 m 阶完全函数，若

$$R(z,a(\alpha))\triangleq\|f^{-1}(z/a(\alpha))\|\quad (5\text{-}2\text{-}12)$$

与 $\alpha\in\tilde{\alpha}_m$ 及 $a(\alpha)\in F_q^{(m)}$ 无关. 这时记

$$R_m(z)=R(z,a(\alpha)).\quad (5\text{-}2\text{-}12a)$$

定理 1　$f(x^{(n)})$ 为 m 阶相关免疫的充要条件为 $f(x^{(n)})$是 m 阶完全函数.

证明　先证充分性. 若 $f(x^{(n)})$为 m 阶完全函数，则对于任何 $\alpha\in\tilde{\alpha}_m$, $x(\alpha)\in F_q^{(m)}$,

$$p_z(z)=P_r\{Z=z\}$$
$$\overset{*}{=}\sum_{a'(\alpha)\in F_q^{(m)}}P_r\{X(\alpha)=a'(\alpha),\ Z=z\}$$
$$\overset{*}{=}\sum_{a'(\alpha)\in F_q^{(m)}}P_r\{X(\alpha)=a'(\alpha)\}\cdot P_r\{Z=z/X(\alpha)=a'(\alpha)\}$$
$$\overset{*}{=}\sum_{a'(\alpha)\in F_q^{(m)}}P_r\{X(\alpha)=a'(\alpha)\}\cdot\left[-\frac{(z,a'(\alpha))}{q^{n-m}}\right]$$
$$\overset{*}{=}\frac{R_m(z)}{q^{n-m}},$$

而

$$p(x(\alpha),z)\overset{*}{=}P_r\{X(\alpha)=x(\alpha),Z=z\}$$
$$\overset{*}{=}P_r\{X(\alpha)=x(\alpha)\}\cdot P_r\{Z=z/X(\alpha)=x(\alpha)\}$$
$$\overset{*}{=}-\frac{R_m(z)}{q^n},$$
$$p_X(x(\alpha))=P_r\{X(\alpha)=x(\alpha)\}\overset{*}{=}q^{-m},$$

因此有

$$p(x(\alpha),z)\overset{*}{=}p_X(x(\alpha))p_z(z)$$

对任何 $\alpha\subset\tilde{\alpha}_m$，$x(\alpha)\in F_q^{(m)}$，$z\in F_q$ 成立，此即 $f(x^{(n)})$ 为 m 阶相关免疫函数。

反之，若 $f(x^{(n)})$ 为 m 阶相关免疫函数，则对任何 $\alpha\in\tilde{\alpha}_m$，$x(\alpha)\in F_q^{(m)}$，$z\in F_q$，有(5-2-4)成立，这时有

$$p_z(z)\overset{*}{=}\frac{p(x(\alpha),z)}{p_X(x(\alpha))}=P_r\{Z=z/X(\alpha)=x(\alpha)\}$$
$$\overset{*}{=}P_r\{x(\alpha^c)\in f^{-1}(z/x(\alpha))\}$$
$$\overset{*}{=}\frac{1}{q^{n-m}}\|f^{-1}(z/x(\alpha))\|\overset{*}{=}\frac{R(z,x(\alpha))}{q^{n-m}}$$

成立，因此

$$R(z,x(\alpha))\overset{*}{=}p_z(z)\cdot q^{n-m}$$

与 $a\in\tilde{\alpha}_m$，$x(\alpha)\in F_q^{(m)}$ 无关，此即 $f(x^{(n)})$ 为 m 阶完全函数，必要条件成立。定理得证。

定理 1 给出了相关免疫函判别的一个等价条件，由 $f(x^{(n)})$ 的完全性可直接给出 $f(x^{(n)})$的相关免疫性。

例 1　若 $f(x^{(n)})$为线性函数，即

$$f(x^{(n)}) = \beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n, \qquad (5\text{-}2\text{-}13)$$

且 $\beta_1, \cdots, \beta_n$ 均不为 0，则 $f(x^{(n)})$为相关免疫函数。

证明　对任何 $\alpha \in \tilde{\alpha}_{n-1}$，均可将 α 表示为 N_i，这时对任何 $i = 1, 2, \cdots, n$，与任何 $a(N_i) \in F_q^{(n-1)}$，

$$f(x_i, a(N_i)) = \beta_0 + \beta_i x_i + \sum_{i' \neq i} a_{i'} \beta_{i'}$$

为一个 $F_q \to F_q$ 的 1-1 映射，因此对任何 $z \in F_q$，

$$R_{n-1}(z) = \| f^{-1}(z/a(N_i)) \| = 1$$

与 $i = 1, \cdots, n$，$a(N_i) \in F_q^{(n-1)}$ 无关，此即 $f(x^{(n)})$ 为 $n-1$ 阶完全函数或 $n-1$ 阶相关免疫函数。

在 $q = 2$ 时，本例的逆命题也成立，即任何相关免疫函数必为(5-2-13)的线性函数，且 $\beta_i \neq 0$，$i = 1, 2, \cdots, n$。对此命题在以后证明。

例 2　若

$$f(x^{(n)}) = x_1 x_2 \cdots x_n,$$

则 $f(x^{(n)})$ 不为一阶相关免疫函数。

证明　对任何 $\alpha \in \tilde{\alpha}_1$，可记 $\alpha = \{i\}$，因此 $a(\alpha) = a_i$，这时对任何 $i = 1, 2, \cdots, n$，$a_i \in F_q$，总有

$$\| f(z = 0/a_i) \| \overset{*}{=} \begin{cases} q^{n-1}, & \text{若 } a_i = 0, \\ q^{n-1} - (q-1)^{n-1}, & \text{若 } a_i \neq 0, \end{cases}$$

因此 $f(x^{(n)})$为一阶不完全函数，也是一阶不相关免疫函数。

定义 4　设 $f_i(x^{(k)})$，$i = 1$，2 为 $F_q^{(k)} \to F_q^s$ 的两个非线性组合函数，若对任何 $z \in F_q$，有

$$\| f_1^{-1}(z) \| = \| f_2^{-1}(z) \|$$

成立，则称 $f_1(\cdot)$，$f_2(\cdot)$为两个 q 元函数，且分布等价。如$\mathcal{F}$为一

个 $F_q^{(k)} \to F_q$ 的函数类，它们的元分布等价，则称 $\mathscr{F}$ 为一个 q 元分布等价类。

以下对 $f(x^{(n)})$ 函数记

$$\mathscr{F}_m[f(x^{(n)})]=\{f[x(\alpha^c),a(\alpha)]:\alpha\in\tilde{\alpha}_m,\ a(\alpha)\in F_q^{(m)}\},\tag{5-2-14}$$

为由 $f(x^{(n)})$ 产生的 $n-m$ 元函数类，其中 $0\leqslant m\leqslant n-1$，若 $m=0$，则 $\mathscr{F}_m[f(x^{(n)})]=\{f(x^{(n)})\}$。

定理 2 以下条件相互等价：

(i) $f(x^{(n)})$ 为 m 阶完全函数；

(ii) 对任何 $0\leqslant k\leqslant m$，$\mathscr{F}_k[f(x^{(n)})]$ 是一个 $m-k$ 阶完全且为 $n-k$ 元分布等价类；

(iii) 有一个 k，$0\leqslant k\leqslant m$，$\mathscr{F}_k[f(x^{(n)})]$ 为 $m-k$ 阶完全且 $n-k$ 元分布等价类。

证明 该定理证明由完全函数的定义及分布等价类定义即得，证明过程为(i)⇒(ii)⇒(iii)⇒(i)。

利用定理 2 也可对 $f(x^{(n)})$ 的相关免疫性进行判别。

若 x_i 在 $f(x_1,\cdots,x_n)$ 中不出现，或对任何 $x(N_i)\in F_q^{(n-1)}$，x_i，$x_i'\in F_q$，总有

$$f(x(N_i),x_i)=f(x(N_i),x_i'),$$

则称 $f(x^{(n)})$ 与 x_i 无关，同样可定义 $f(x^{(n)})$ 与 $x(\alpha)$ 无关。

引理 2 若 $f(x^{(n)})$ 与 $x(\alpha)$ 无关，则 $f(x^{(n)})$ 为 $n-\|\alpha\|$ 阶不完全函数。

证明 因为 $f(x^{(n)})$ 与 $x(\alpha)$ 无关，因此有

$$f(x^{(n)})=f(x(\alpha^c))$$

成立。这时 $z=f(x^{(n)})=f(x(\alpha^c))$ 与 $x(\alpha^c)$ 不相互独立，$f(x^{(n)})$ 不为 $n-\|\alpha\|$ 阶相关免疫或 $n-\|\alpha\|$ 阶不完全函数。引理得证。

2.3　关于完全函数的若干性质

为简单起见，本段只讨论 $q=2$ 的情形，这时非线性组合函数可表示为

$$f(x^{(n)})=\sum_{\alpha\subset N}c_\alpha\Big[\prod_{i\in\alpha}x_i\Big],\qquad(5\text{-}2\text{-}15)$$

其中 $c_\alpha=0$ 或 1 为 $\prod\limits_{i\in\alpha}x_i$ 项的系数，我们称 $\|\alpha\|$ 为 $\prod\limits_{i\in\alpha}x_i$ 的次数，而称

$$\partial^0 f(x^{(n)})=\mathrm{Max}\{\|\alpha\|:c_\alpha=1\}\qquad(5\text{-}2\text{-}16)$$

为 $f(x^{(n)})$ 的次数。显然有

$$0\leqslant\partial^0 f(x^{(n)})\leqslant n$$

成立。记

$$R_i=R_i[f(x^{(n)})]=\|A_i[f(x^{(n)})]\|,\ i=0,1,\qquad(5\text{-}2\text{-}17)$$

其中 $A_i[f(\cdot)]$ 为 $f(\cdot)$ 的组合表示。这时显然有 $R_0+R_1=2^n$，我们称 $f(x^{(n)})$ 为一个 (R_0,R_1) 型函数。

引理 3　若 $\partial^0 f(x^{(n)})=n$，则 $R_i[f(x^{(n)})]$ 为奇数，否则为偶数。

证明　用归纳法证。当 $n=1$ 时，若 $\partial^0 f(x^{(n)})=1$，则 $f(x^{(n)})=f(x)=\beta_0+x$，这时必有 $(R_0,R_1)=(1,1)$ 成立；若 $\partial^0 f(x^{(n)})<1$，则 $f(x^{(n)})=f(x)=\beta_0$，因此 $(R_0,R_1)=(0,2)$ 或 $(2,0)$，所以引理的结论成立。

现假定引理 3 的命题对 n 成立，证明对 $n+1$ 时也成立。记

$$f(x^{(n+1)})=(x_{n+1}+1)f_0(x^{(n)})+x_nf_1(x^{(n)}),$$

若 $\partial^0 f(x^{(n+1)})=n+1$，则有

(i)　若 $\partial^0 f_0(x^{(n)})=n$，则 $\partial^0 f_1(x^{(n)})<n$；

(ii)　若 $\partial^0 f_0(x^{(n)})<n$，则 $\partial^0 f_1(x^{(n)})=n$。

对情形(i)，由归纳法有

$R_0[f_0(x^{(n)})]=$ 奇数，$R_0[f_1(x^{(n)})]=$ 偶数，因为

$$A_0[f(x^{(n+1)})]$$
$$=A_0[f_0(x^{(n)})]\otimes(x_{n+1}=0)\bigcup A_0[f_1(x^{(n)})]\otimes(x_{n+1}=1),$$

所以

$$R_0[f(x^{(n+1)})]=R_0[f_0(x^{(n)})]+R_0[f_1(x^{(n)})]$$

为奇数。同理，对情形(ii)有

$R_0[f_0(x^{(n)})]$=偶数，$R_0[f_1(x^{(n)})]$=奇数，

$R_0[f(x^{(n+1)})]=R_0[f_0(x^{(n)})]+R_0[f_1(x^{(n)})]$=奇数。

如果 $\partial^0 f(x^{(n+1)})<n+1$. 则必有

(iii) 若 $\partial^0 f_0(x^{(n)})=n$，则 $\partial^0 f_1(x^{(n)})=n$；

(iv) 若 $\partial^0 f_0(x^{(n)})<n$，则 $\partial^0 f_1(x^{(n)})<n$，

因此 $R_0[f_0(x^{(n)})]$与 $R_0[f_1(x^{(n)})]$同时为奇数((iii)的情形)，或同时为偶数((iv)的的情形)，这时 $R_0[f(x^{(n+1)})]$必为偶数，引理的结论对 $n+1$ 时也成立。证毕。

定理 8 如 $\partial^0 f(x^{(n)})=k$，$0<k\leqslant n$，则 $f(x^{(n)})$为 $n-k+1$ 阶不完全函数。

证明 不失一般性，我们设 $x_1\cdots x_k$ 项的系数不为 0，记

$$f(x^{(n)})=f_{\mathrm{I}}(x^{(n)})+f_{\mathrm{II}}(x^{(n)}),$$

其中 $f_{\mathrm{I}}(x^{(n)})$为 $x_1,\cdots,x_k$ 的函数，$f_{\mathrm{II}}(x^{(n)})$ 中每一项都有 $x_{k+1},\cdots,x_n$ 的因子，因此当 $x_{k+1}=\cdots=x_n=0$ 时，

$$f(x^{(n)})=f_1(x^{(k)}),$$

且有 $\partial^0 f(x^{(n)})=\partial^0 f_{\mathrm{I}}(x^{(k)})=k$. 因此 $f_1(x^{(k)})$ 是一阶不完全的，这时存在两个 $a_i,a_i'\in F_2$，$1\leqslant i<i'\leqslant k$，使

$$\|f_{\mathrm{I}}^{-1}(0/a_i)\|\neq\|f_{\mathrm{I}}^{-1}(0/a_i')\|$$

成立，此即

$$\|f^{-1}(0/x_{i'}=a_{i'},x_{k+1}=\cdots=x_n=0)\|$$
$$\neq\|f^{-1}(0/x^{i'}=a^{i''},x_{k+1}=\cdots=x_n=0)\|,$$

这就是 $f(x^{(n)})$为 $n-k+1$ 阶不完全函数。定理得证。

推论 当 $q=2$ 时，$f(x^{(n)})$为完全函数的充要条件为

$$f(x^{(n)})=\beta_0+x_1+x_2+\cdots+x_n,\ \beta_0\in F_2。\qquad(5\text{-}2\text{-}18)$$

证明 充分性在本节例 1 中已证，必要性由上面定理 3 即得。因为若 $\partial^0 f(x^{(n)})\geqslant 2$，则 $f(x^{(n)})$ 必为 $n-1$ 阶不完全函数，

因此若 $f(x^{(n)})$为完全函数，则必有 $\partial^0 f(x^{(n)}) \leqslant 1$。另一方面，由本节引理 2 知，$f(x^{(n)})$与任何 x_i 均相关（即 x_i 在 $f(x^{(n)})$ 中必出现），因此(5-2-18)必成立。

在(5-2-12)中，我们已对 $R(z, a(\alpha))$进行了定义。在 $q=2$ 的情形，记

$$R_i(a(\alpha)) = R(i, a(\alpha)), i = 0, 1, \qquad (5\text{-}2\text{-}19)$$

对任何固定的 $\alpha \in \tilde{\alpha}_m$，有

$$R_i[f(x^{(n)})] = \sum_{a(\alpha) \in F_2^{(m)}} R_i(a(\alpha)), \qquad (5\text{-}2\text{-}20)$$

因此有

定理 4　$f(x^{(n)})$为 m 阶相关免疫函数的必要条件是

$$R_i[f(x^{(n)})] = 2^m \cdot R'_i, i = 0, 1, \qquad (5\text{-}2\text{-}21)$$

其中 $R'_i, i = 1, 2$，为两个正整数，$R'_0 + R'_1 = 2^{n-m}$。

证明　该定理由(5-2-20)、m 阶完全函数定义及本节定理 1 即得。

2.4　相关免疫函数的递推构造性质

以下记 $f_i(x^{(n)}), i = 0, 1$ 为两个 n 元函数，并称 $f(x^{(n+1)})$ 为 $f_i(x^{(n)})(i = 0, 1)$的结合，若

$$f(x^{(n+1)}) = (x_{n+1} + 1) f_0(x^{(n)}) + x_{n+1} f_1(x^{(n)}), \qquad (5\text{-}2\text{-}22)$$

且记为

$$f(x^{(n+1)}) = f_0(x^{(n)}) \vee f_1(x^{(n)}). \qquad (5\text{-}2\text{-}23)$$

所谓相关免疫函数的递推性质，就是由 $f_i(x^{(n)})$的相关免疫性讨论 $f(x^{(n+1)})$的相关免疫性。

设 $f_i(x^{(n)})(i = 0, 1)$是两个(n, m)阶相关免疫函数，则它们的 $R(z, a(\alpha))$(见 (5-2-12)的定义)分别为

$$R(z, a(\alpha), i) = R_m(z, i), i = 0, 1. \qquad (5\text{-}2\text{-}24)$$

它们与 $\alpha \in \tilde{\alpha}_m, a(\alpha) \in F_2^{(m)}$ 无关。这时我们称 $f_i(x^{(n)})$ 是 (R_0, R_1)型。若

$$R_m(j, i) = R_j,\ j = 0, 1, \tag{5-2-25}$$

记全体 (n, m) 阶，(R_0, R_1) 型函数为 $\mathscr{F}_{n,m}(R_0, R_1)$，其中 $R'_0 + R'_1 = 2^{n-m}$，$R_i = 2^m R'_i$，$i = 0, 1$。

关于(5-2-22)的结合定义，也可以推广到任何变量 x_t。若记 $f_{ij}(x(N'_i))$，$j = 0, 1$ 为两个 n 元函数，其中

$$N'_i = \{1, 2, \cdots, n+1\} - \{i\} = \{1, \cdots, i-1, i+1, \cdots, n+1\}.$$

这时称

$$f(x^{(n+1)}) = (x_t + 1) f_{t0}(x(N'_i)) + x_t f_{t1}(x(N'_i)) \tag{5-2-26}$$

为 $f_{ij}(x(N'_i))$关于变量 x_t 的结合，并记为

$$f(x^{(n+1)}) = f_{t0}(x(N'_i)) \vee f_{t1}(x(N'_i)). \tag{5-2-27}$$

因此，(5-2-22)的定义实际上是(5-2-26)的特例。如 $f(x^{(n+1)})$是 $f_{ij}(x(N'_i))$ 的结合，则称 $f_{ij}(x(N'_i))$，$j = 0, 1$ 为 $f(x^{(n+1)})$ 在 x_t 元上的分解。

定理 5 若 $f_j(x^{(n)}) \in \mathscr{F}_{n,m}(R_0, R_1)$，$j = 0, 1$，则它们的结合 $f(x^{(n+1)})$必为 $\mathscr{F}_{n+1,m}(2R_0, 2R_1)$函数。

证明 对任何一组 $\alpha = \{i_1, \cdots, i_m\} \in \tilde{\alpha}'_m$ 及任何 $a(\alpha) \in F_2^{(m)}$，我们计算

$$\| f^{-1}(z/a(\alpha)) \|$$

的值。上述 $\tilde{\alpha}'_m$为全体 $1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n+1$的 α 集合，这时有以下情形发生。

(i) 若 $i_m = n+1$，则 $a_{i_m} = a_{n+1}$，且有

$$\| f^{-1}(z/a(\alpha)) \| = \begin{cases} \| f_1^{-1}(z/a(\alpha')) \|, & \text{若 } a_{n+1} = 1, \\ \| f_1^{-0}(z/a(\alpha')) \|, & \text{若 } a_{n+1} = 0, \end{cases} \tag{5-2-28}$$

其中 $\alpha' = \{i_1, i_2, \cdots, i_{m-1}\}$。

(ii) 若 $i_m < n+1$，这时

$$\| f^{-1}(z/a(\alpha)) \| = \| \{x(\alpha^c) : f(x(\alpha^c), a(\alpha)) = z\} \|$$

$$= \sum_{\varepsilon_{n+1}=0}^{1} \| \{x(\alpha^c) : x_{n+1} = a_{n+1}, f(x(\alpha^c), a(\alpha)) = z\} \|$$

$$=\|f_0^{-1}(z/a(\alpha))\|+\|f_1^{-1}(z/a(\alpha))\|。\qquad(5\text{-}2\text{-}29)$$

现比较(5-2-28)和(5-2-29)的结果。取

$$i\notin\{i_1,\cdots,i_{m-1},n+1\},$$

这时有

$$\|f_j^{-1}(z/a(\alpha'))\|\overset{*}{=}\sum_{a_i=0}^{1}\|f_j^{-1}(z/a(\alpha'),a_i)\|$$

对任何 $j=0,1$ 成立。由定理条件知

$$\|f_j^{-1}(z/a(\alpha'),a_i)\|=R_z,\ j=0,1$$

成立，因此(5-2-28)、(5-2-29)右边的值均为 $2R_z$，$z=0,1$，它们与 $\alpha\in\tilde{\alpha}'_m$，$a(\alpha)\in F_2^{(m)}$ 无关，因此必有

$$f(x^{(n+1)})\in\mathscr{F}_{n+1,m}(2R_0,2R_1)$$

成立。定理得证。

由本节定理 5 可递推构造 $\mathscr{F}_{n+1,m}$ 类的函数，即任取 $f_0(x^{(n)})$，$f_1(x^{(n)}\in\mathscr{F}_{n,m}(R_0,R_1)$，则它们的结合 $f(x^{(n+1)})$ 必为 $\mathscr{F}_{n+1,m}$ 函数。定理 5 的逆命题不一定成立，因为若 $f(x^{(n+1)})$ 为 $n+1$，m 阶函数，它的分解可能为两个 $(n,m-1)$ 阶函数。

例 3　利用定理 6 构造 $\mathscr{F}_{6,2}$ 的函数。

解　(1) 由完全函数的定义直接构造 $\mathscr{F}_{4,2}$ 函数为

$$f(x^{(4)})=\beta_0+x_1+x_2+x_3,\ \beta_0=0,1。$$

如我们记 SYM(k) 为 $\{1,2,\cdots,k\}$ 上的置换群，则对任何 $\tau\in$SYM(4)，

$$\tau[f(x^{(4)})]=\beta_0+x_{\tau(1)}+x_{\tau(2)}+x_{\tau(3)}$$

均为 $\mathscr{F}_{4,2}(2,2)$ 函数。

(2) 任取 $f_0(x^{(4)})$，$f_1(x^{(4)})$ 为(1)中的两个函数，如

$$f_0(x^{(4)})=x_1+x_2+x_3,\ f_1(x^{(4)})=x_1+x_3+x_4,$$

作 $f_0(x^{(4)})$ 与 $f_1(x^{(4)})$ 的结合，这时

$$f(x^{(5)})=x_1+x_2+x_3+x_3x_5+x_4x_5$$

及任何

$$\beta_0+\tau[f(x^{(5)})],\beta_0=0,1;\tau\in \mathrm{SYM}(5) \qquad (5\text{-}2\text{-}30)$$

均为 $\mathscr{F}_{5,2}(4,4)$类函数.

(3) 任取(5-2-30)的两个元,如

$$f_0(x^{(5)})=x_1+x_2+x_3+x_3x_5+x_4x_5,$$

$$f_1(x^{(5)})=x_1+x_2+x_5+x_3x_4+x_3x_5,$$

这时它们结合函数

$$f(x^{(6)})=x_1+x_2+x_3+x_3x_5+x_4x_5+x_3x_6+x_5x_6+x_3x_4x_6+x_4x_5x_6$$

及全体

$$\beta_0+\tau[f(x^{(6)})],\ \beta_0=0,1,\tau\in \mathrm{SYM}(6),$$

均为 $\mathscr{F}_{6,2}(8,8)$类函数.

2.5 关于熵漏的计算公式

由(5-2-17)知,若 $f(x^{(n)})$为(R_0,R_1)型函数,则必有

$$p_z(z)\overset{*}{=}\frac{R_z}{2^n}\overset{\triangle}{=}\begin{cases}\varepsilon, & \text{若 } z=0,\\ 1-\varepsilon, & \text{若 } z=1.\end{cases} \qquad (5\text{-}2\text{-}31)$$

这时熵漏的计算公式为

$$\mathscr{E}_0[f(x^{(n)})]=1-h(\varepsilon), \qquad (5\text{-}2\text{-}32)$$

其中 $h(\varepsilon)\overset{*}{=}-\varepsilon\log\varepsilon-(1-\varepsilon)\log(1-\varepsilon)$.同样,我们有 z 关于$X(\alpha)=a(\alpha)$的条件分布为

$$p(z/a(\alpha))\overset{*}{=}\frac{R_z[a(\alpha)]}{2^{n-m}}\overset{\triangle}{=}\begin{cases}\varepsilon[a(\alpha)], & \text{若 } z=0,\\ 1-\varepsilon[a(\alpha)], & \text{若 } z=1.\end{cases} \qquad (5\text{-}2\text{-}33)$$

因此 m 阶熵漏的计算公式为

$$\mathscr{E}_m[f(x^{(n)})]\overset{*}{=}\max_{a\in\tilde{\alpha}_m}[1-E\{h[\varepsilon(X(\alpha))]\}], \qquad (5\text{-}2\text{-}34)$$

其中

$$h[\varepsilon(X(\alpha))]\overset{*}{=}-\varepsilon(X(\alpha))\log\varepsilon(X(\alpha))-[1-\varepsilon(X(\alpha))]\log[1-\varepsilon(X(\alpha))]$$

为随机变量,$E\{h(\cdot)\}$为 $h(\cdot)$的数学期望.

定理 6　(i) $f(x^{(n)})$无熵漏的充要条件为

$$R_0 = R_1 \overset{*}{=} 2^{n-1};$$

(ii) $f(x^{(n)})$ 无 m 阶熵漏的充要条件为对任何$i=0$，1，$\alpha\in\tilde{\alpha}_m, a(\alpha)\in F_2^{(m)}$，

$$R_i[a(\alpha)] \overset{*}{=} 2^{n-m-1}.$$

证明　由关系式(5-2-33)、(5-2-34) 及熵函数$h(\varepsilon)=1$的充要条件为 $\varepsilon \overset{*}{=} \frac{1}{2}$的性质即得。

由定理 6 知，无 m 阶熵漏的条件比 m 阶相关免疫性条件要求更高，它不仅要求 $R[z, a(\alpha)]$与 $\alpha\in\tilde{\alpha}_m$，$a(\alpha)\in F_2^{(m)}$ 无关，且要求与 z 无关，即在(5-2-12a)中要求

$$R_m(0) = R_m(1) \overset{*}{=} 2^{n-m-1} \qquad (5\text{-}2\text{-}35)$$

成立，因此，寻找 m 阶无熵漏的函数只要在 m 阶相关免疫函数中寻找，使(5-2-35)成立，对此我们不再作单独研究。

§3　相关免疫函数的组合构造

3.1　完全函数的组合表示

在上一节中给出了相关免疫函数的判别性质，以及由 $\mathscr{F}_{n,m}$ 递推构造 $\mathscr{F}_{n+1,m}$ 的性质。由上一节的结果还不能构造全部 $\mathscr{F}_{n+1,m}$ 函数，因为一些 $\mathscr{F}_{n+1,m}$ 函数可由 $\mathscr{F}_{n,m-1}$ 的函数结合产生。现在进一步利用组合表示讨论它们的构造问题。为了简单起见，仍只讨论 $q=2$ 的情形，这时任何 F_2 上的 n 元函数 $f(x^{(n)})$组合表示为

$$A_0[f(x^{(n)})] = \{x^{(n)} : f(x^{(n)}) = 0\}. \qquad (5\text{-}3\text{-}1)$$

若我们把集合 A_0 的向量作为行向量排成一个矩阵，它的行互不相同，且列数为 A_0 的元素个数$\|A_0\|$，这个矩阵称为 $f(x^{(n)})$ 的组合矩阵，且仍记为 $A_0[f(x^{(n)})]$。这样，任何一个非线性组合函数均可表示为一个组合矩阵。以下记 $A^{(n)}$ 为 F_2 上的 $r\times n$ 矩阵，即

$$A^{(n)}=\begin{bmatrix} a_{11}, a_{12}, \cdots, a_{1n} \\ a_{21}, a_{22}, \cdots, a_{2n} \\ \cdots\cdots\cdots\cdots\cdots \\ a_{r1}, a_{r2}, \cdots, a_{rn} \end{bmatrix}, \tag{5-3-2}$$

其中 $a_{ij}\in F_2$，现在对列向量 $a_{\cdot j}=\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{rj} \end{bmatrix}$，我们定义

$$\theta_j\{(0)\}=\{i: a_{ij}=0\},\ j=1, 2, \cdots, n, \tag{5-3-3}$$

其中 $$\theta_j(1)=\{1,\cdots,r\}/\theta_j(0)=\{i: a_{ij}=1\}。 \tag{5-3-3a}$$

以下对任何 $\theta\subset\{1, 2, \cdots, r\}$。记 $A^{(n)}(\theta)$ 为 $A^{(n)}$ 的子矩阵，它由 $A^{(n)}$ 中 θ 的行构成，因此矩阵 $A^{(n)}[\theta_j(0)]$，$A^{(n)}[\theta_j(1)]$ 在第 j 列的元分别为 0 或 1。现对任何 $\alpha\in\tilde{\alpha}_m, a(\alpha)\in F_2^{(m)}$，我们记

$$\theta[a(\alpha)]=\bigcap_{t\in\alpha}\theta_j\ (aa_j), \tag{5-3-4}$$

其中 $\alpha=(j_1, \cdots, j_m)$，$a(\alpha)=(a_{j_1}, \cdots, a_{j_m})$，这时矩阵 $A^{(n)}\{\theta[a(\alpha)]\}$ 在 j_i 列上的元为 a_{j_i}，且记 $\|A^{(n)}(\theta)\|$ 为矩阵 $A^{(n)}(\theta)$ 的行数，这时有

定理 1 $f(x^{(n)})$ 为 (n, m) 阶相关免疫函数的充要条件为它的组合矩阵 $A_0^{(n)}=A_0[f(x^{(n)})]$ 对任何 $\alpha\in\tilde{\alpha}_m$，$a(\alpha)\in F_2^{(m)}$，

$$\|A_0^{(n)}\{\theta[a(\alpha)]\}\|=R_{m,0} \tag{5-3-5}$$

与 α，$a(\alpha)$ 无关。

证明 由 m 阶相关免疫性与 m 阶完全函数的等价性即得。

使(5-3-5)成立，且各行互不相同的 $r\times n$ 阶矩阵 A，我们称之为 (n, m, r) 阶完全矩阵。为构造 $\mathscr{F}_{n,m}(r)$ 函数，只要构造 (n, m, r) 矩阵即可。这里

$$\mathscr{F}_{n,m}(r)=\{f(x^{(n)})\in\mathscr{F}_{n,m}: \|A_0[f(x^{(n)})]\|=r\}。 \tag{5-3-6}$$

若 A, B 是两个 $r\times n$ 阶矩阵，分别为

$$A=[a_{ij}]_{r\times n},\ B=[b_{ij}]_{r\times n},$$

记 $C=(A,B)_{n+1}$ 为 A, B 在 $n+1$ 列上的结合，若

$$C=\begin{bmatrix} a_{11} & a_{12}\cdots a_{1n} & 0\\ a_{21} & a_{22}\cdots a_{2n} & 0\\ \cdots\cdots & \cdots\cdots & \\ a_{r1} & a_{r2}\cdots a_{rn} & 0\\ b_{11} & b_{12}\cdots b_{1n} & 1\\ b_{21} & b_{22}\cdots b_{2n} & 1\\ \cdots\cdots & \cdots\cdots & \\ b_{r1} & b_{r2}\cdots b_{rn} & 1 \end{bmatrix},\qquad (5\text{-}3\text{-}7)$$

显然有

引理 1　若 $f_0(x^{(n)})$, $f_1(x^{(n)})$ 的组合矩阵分别为 A, B, 则 $f(x^{(n+1)})$ 为 $f_0(x^{(n)})$, $f_1(x^{(n)})$ 结合的充要条件为

$$A_0[f(x^{(n+1)})]=(A,B)_{n+1}.\qquad (5\text{-}3\text{-}8)$$

证明略.

由本节定理 1 知，为构造 $\mathscr{F}_{n,m}(r)$ 函数，只要构造 (n,m,r) 型矩阵即可.以下我们把矩阵 A 中行向量的置换看作同一矩阵，因为 $f(x^{(n)})$ 的组合表示与 $A_0[f(x^{(n)})]$ 中元的次序无关. 另外有

引理 2　若 A 为 (n,m,r) 型矩阵，有

(i) 若记 $\tau\in \mathrm{SYM}(n)$, 且 $\tau[A]$ 为矩阵 A 中列的 τ 置换，则 $\tau[A]$ 也是 (n,m,r) 型矩阵.

(ii) $\bar{A}=[\bar{a}_{ij}]_{r\times n}$ 也是 (n,m,r) 型矩阵.

证明　性质(i)由

$$[\tau(A)]\{\theta[a(\alpha)]\}=\tau[A\{\theta[a(\tau^{-1}(\alpha))]\}]$$

即得，其中 τ^{-1} 为 τ 的逆置换，而

$$\tau^{-1}(\alpha)=\{\tau^{-1}(i),\ i\in\alpha\},$$

这时由(5-3-5)式可得对任何 $\alpha\in\tilde{\alpha}_m$，$a(\alpha)\in F^{\binom{m}{2}}$，必有 $\tau^{-1}(\alpha)\in\tilde{\alpha}_m$，且

$$\|[\tau(A)]\{\theta[a(\tau^{-1}(\alpha))]\}\|=\|\tau[A\{\theta[a(\tau^{-1}(\alpha))]\}]\|$$
$$=\|\tau[A\{\theta[a(\tau^{-1}(\alpha))]\}]\|=R_{m,0}, \qquad (5\text{-}3\text{-}9)$$

此即 $\tau(A)$为(n, m, r)型矩阵。

对性质(ii)，同样由

$$(\bar{A})\{\theta[a(\alpha)]\}=\overline{A\{\theta[\bar{a}(\alpha)]\}}$$

即得，其中 $\bar{a}(\alpha)=(\bar{a}_i, i\in\alpha)$，这时仿(5-3-9)的推导过程可证得，引理得证。

关于此引理我们还可得到更多的结论，如 α 为 $\{1,\cdots,n\}$中的任何子集，记矩阵 A 的列向量为 $a_{\cdot j}$，$j=1,\cdots,n$，及

$$A(\alpha)=[a_{\cdot j}, j\in\alpha]$$

为矩阵 A 的部分列向量，则矩阵 A 可表示为

$$A=[A(\alpha), A(\alpha^c)]$$

的形式，且定义

$$D_\alpha(A)=[\bar{A}(\alpha), A(\alpha^c)]$$

为 A 的部分列的新运算，其中

$$\bar{A}(\alpha)=[\bar{a}_{\cdot j}, j\in\alpha].$$

于是有

引理 3 若 A 为(n, m, r)型矩阵，则对任何 $\alpha\subset\{1,\cdots,n\}$，$D_\alpha[A]$也是$(n, m, r)$型矩阵。

此引理的证明与本节引理 2 中(ii)相似。对固定矩阵A，我们称

$$\tilde{A}=\{\tau[D_\alpha(A)]:\alpha\supset N, \tau\in\mathrm{SYM}(n)\} \qquad (5\text{-}3\text{-}10)$$

为一个 A 类矩阵，这时有

定理 2 若 A 是一个(n, m, r)型矩阵，则任何 A 类矩阵都是(n, m, r)型矩阵。

证明 由本节引理 2 和 3 即得。

推论 若 A，B 是两个 $r\times(n-1)$ 矩阵，它们的结合 $C=$

$(A,B)_n$为$(n,m,2r)$型矩阵，则对任何$\alpha\supset\{1,\cdots,n-1\}$，$\tau\in SYM(n-1)$，

$$\tau[D_\alpha(C)]=(\tau[D_\alpha(A)],\tau[D_\alpha(B)])_n$$

也是$(n,m,2r)$型矩阵。

由该定理知，如能构造一个(n,m,r)型矩阵A，就可构造一类$\tilde{A}$矩阵。

3.2　矩阵的对偶性

为讨论$\mathscr{F}_{n,m}$函数的递推构造，我们先讨论矩阵的对偶性质。

定义　(i) 称两个(n,m,r)型矩阵A，B为对偶的，若对任何$\alpha\in\tilde{\alpha}_m$，$a(\alpha)\in F_2^{(m)}$，$j\notin\alpha$，$a_j\in F_2$，总有

$$\|A\{\theta[a(\alpha),a_j]\}\|=\|B\{\theta[a(\alpha),a_i]\}\| \qquad (5\text{-}3\text{-}11)$$

成立，其中$\theta[a(\alpha),a_j]=\theta[a(\alpha)]\cap\theta_j(a_j)$。

(ii)　在本定义(i)中，称A，B为反对偶的，若

$$\|A\{\theta[a(\alpha),a_j]\}\|\overset{*}{=}r-\|B\{\theta[a(\alpha),a_j]\}\|$$
$$=\|B\{\theta[a(\alpha),\bar{a}_j]\}\|. \qquad (5\text{-}3\text{-}11a)$$

有时简称对偶(或反对偶)的(n,m,r)型矩阵为m阶对偶(或反对偶)矩阵。

定理3　两个(n,m,r)阶矩阵A，B的结合$C=(A,B)_{n+1}$为$(n+1,m+1,r)$阶矩阵的充要条件为A，B是两个m阶反对偶矩阵。

证明　若A，B是m阶反对偶的，则对任何$\alpha=\{j_1,j_2,\cdots,j_{m+1}\}$，$a(\alpha)\in F_2^{(m+1)}$，估计$\|C\{\theta[a(\alpha)]\}\|$的值。对此有以下两种情形，即

(1)　若$j_{m+1}=n+1$，则

$$\|C\{\theta[a(\alpha)]\}\|=\begin{cases}\|A\{\theta[a(\alpha')]\}\|, & \text{若 } a_{n+1}=0,\\ \|B\{\theta[a(\alpha')]\}\|, & \text{若 } a_{n+1}=1,\end{cases}$$

其中$\alpha'=\{j_1,\cdots,j_m\}\in\tilde{\alpha}_m$。这时有

$$\|C\{\theta[a(\alpha)]\}\| = r \tag{5-3-12}$$

成立。

(2) 若 $j_{m+1} < n+1$，则

$$\begin{aligned}\|C\{\theta[a(\alpha)]\}\| &= \|A\{\theta[a(\alpha)]\}\| + \|B\{\theta[a(\alpha)]\}\| \\ &= \|A\{\theta[a(\alpha'), a_{j_{m+1}}]\}\| + \|B\{\theta[a(\alpha'), a_{j_{m+1}}]\}\| \\ &= \|A\{\theta[a(\alpha'), a_{j_{m+1}}]\}\| + \|A\{\theta[a(\alpha'), \bar{a}_{j_{m+1}}]\}\| \\ &= \|A\{\theta[a(\alpha')]\}\| = r,\end{aligned}$$

因此 $C = (A,B)_{n+1}$ 为 $(n+1, m+1, r)$型矩阵。

关于定理 3 的逆命题：若 C 为$(n+1, m+1, r)$型矩阵，则对任何 $\alpha \in \tilde{a}_{m+1}, a(\alpha) \in F_2^{(m+1)}$，总有 $\|C\{\theta[a(\alpha)]\}\| = r$ 成立。若取 $j_{m+1} < n+1$，这时。

$$\|C\{\theta[a(\alpha)]\}\| \overset{*}{=} \|A\{\theta[a(\alpha)]\}\| + \|B\{\theta[a(\alpha)]\}\| = r \tag{5-3-13}$$

成立。另一方面，记 $a(\alpha) = (a(\alpha'), a_{j_{m+1}})$，这时总有

$$\begin{aligned}\|A\{\theta[a(\alpha')]\}\| &= \|A\{\theta(a(\alpha'), a_{j_{m+1}}]\}\| \\ &+ \|A\{\theta[a(\alpha'), \bar{a}_{j_{m+1}}]\} = r\end{aligned} \tag{5-3-13a}$$

成立，将 (5-3-13a) 与 (5-3-13)相减，即得(5-3-11a) 成立，其中 A, B 为 m 阶反对偶，定理得证。

3.3 $\mathscr{F}_{n,1}$ 函数类的构造

利用上面定理 3 即可构造全部 $\mathscr{F}_{n,1}$ 函数，对此有以下性质。

引理 4 对任何 $r \times n$ 矩阵 A. A 与 $B = \bar{A}$ 总是 0 阶反对偶的。

证明 因为对任何 $j = 1, \cdots, n$, $a \in F_2$,

$$A[\theta_j(a)] = (\bar{B})[\theta_j(a)] = \overline{B[\theta_j(\bar{a})]},$$

必有

$$\|A[\theta_j(a)]\| = \|B[\theta_j(\bar{a})]\|$$

成立，此即 A, B 具有 0 阶反对偶性，引理得证。

以下我们定义 $\sigma=(\sigma_1, \cdots, \sigma_n)$ 为置换向量，$\sigma_j \in \mathrm{SYM}(r)$，对任何 $r\times n$ 阶矩阵

$$B=[b_{\cdot 1}, b_{\cdot 2}, \cdots, b_{\cdot n}],$$

定义

$$\sigma(B)=[\sigma_1(b_{\cdot 1}), \sigma_2(b_{\cdot 2}), \cdots, \sigma_n(b_{\cdot n})],$$

其中 $b_{\cdot j}$ 为列向量，$\sigma_j(b_{\cdot j})$ 为列向量置换，即

$$b_{\cdot j}=\begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{rj} \end{bmatrix},\quad \sigma_j(b_{\cdot j})=\begin{bmatrix} b_{\sigma j(1),\ j} \\ b_{\sigma j(2),\ j} \\ \vdots \\ b_{\sigma j(r),\ j} \end{bmatrix},$$

这时有

引理 5　在引理 4 中，A 与 $\sigma(\bar{A})$ 总是 0 阶反对偶的。

证明略。

以下记 $\tilde{\sigma}(B)$ 为全体 $\sigma(B)$ 矩阵，它们的行互不相同，这样我们就可建立构造全部 $\mathscr{F}_{n,1}(r)$ 函数的运算过程，有关步骤如下：

(1) 对 F_2 上的 $r\times n$ 阶矩阵，按 (5-3-10) 的定义进行分类，在 $\bar{A}$ 类中任取一矩阵 A；

(2) 作矩阵 $B_0=\bar{A}$，且作 $\tilde{\sigma}(B_0)$；

(3) 对固定的 A 及 $B\in\tilde{\sigma}(B_0)$ 作 $C_0=(A, B)_{n+1}$，即为所求的 $(n+1, 1, r)$ 阶矩阵；

(4) 由 C_0 构造

$$\tilde{C}=\{\tau[D_\alpha(C_0)]:\alpha\subset\{1, \cdots, n+1\},\ \tau\in\mathrm{SYM}(n+1)\}$$

为 $(n+1, 1, r)$ 阶矩阵类。

(5) 由 $C\in\tilde{C}$ 作 $A_0[f(x^{(n+1)})]=C$，则 $f(x^{(n+1)})$ 为 $\mathscr{F}_{n+1,1}(r)$ 类函数。

例　试构造全体 $\mathscr{F}_{4,1}$ 类函数。

解　为此，我们只要构造全体 $\mathscr{F}_{4,1}(1, 7)$，$\mathscr{F}_{4,1}(2, 6)$，$\mathscr{F}_{4,1}(3, 5)$，$\mathscr{F}_{4,1}(4, 4)$ 类函数即可。

(1) 对 $\mathscr{F}_{4,1}(1,7)$，我们作

$$A=[0\ 0\ 0\ 0] \text{ 或 } [1\ 0\ 0\ 0],$$

相应的 $\hat{\sigma}(B)=\hat{\sigma}(\bar{A})$为两个单点集

$$\{[1\ 1\ 1\ 1]\},\ \{[0\ 1\ 1\ 1]\},$$

这时$(A,B)_4$为

$$\begin{bmatrix}0&0&0&0\\1&1&1&1\end{bmatrix},\ \begin{bmatrix}1&0&0&0\\0&1&1&1\end{bmatrix}. \tag{5-3-14}$$

它们为两个(4, 1. 2)阶矩阵。

(2) 对 $\mathscr{F}_{4,1}(2,6)$，作 A 矩阵为

$$\begin{bmatrix}0&0&0\\1&1&1\end{bmatrix},\ \begin{bmatrix}0&0&0\\1&1&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\1&0&0\end{bmatrix},$$

相应的 $\hat{\sigma}(\bar{A})$矩阵相同，且均为

$$\left\{\begin{bmatrix}1&1&1\\0&0&0\end{bmatrix},\ \begin{bmatrix}0&1&1\\1&0&0\end{bmatrix},\ \begin{bmatrix}1&0&1\\0&1&0\end{bmatrix},\ \begin{bmatrix}1&1&0\\0&0&1\end{bmatrix}\right\}.$$

这时矩阵

$$\begin{array}{cccccccccccccccc}
0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0\\
1&1&1&0 & 1&1&1&0 & 1&1&1&0 & 1&1&1&0 & 1&1&0&0 & 1&1&0&0\\
1&1&1&1 & 0&1&1&1 & 1&0&1&1 & 1&1&0&1 & 1&1&1&1 & 0&1&1&1\\
0&0&0&1 & 1&0&0&1 & 0&1&0&1 & 0&0&1&1 & 0&0&0&1 & 1&0&0&1
\end{array}$$

$$\begin{array}{cccccccccccccccc}
0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0\\
1&1&0&0 & 1&1&0&0 & 1&0&0&0 & 1&0&0&0 & 1&0&0&0 & 1&0&0&0\\
1&0&1&1 & 1&1&0&1 & 1&1&1&1 & 0&1&1&1 & 1&0&1&1 & 1&1&0&1\\
0&1&0&1 & 0&0&1&1 & 0&0&0&1 & 1&0&0&1 & 0&1&0&1 & 0&0&1&1
\end{array}$$

(5-3-15)

为 12 个(4, 1, 4)阶矩阵。

(3) 对$\mathscr{F}_{4,1}(3,5)$作 A 矩阵为

$$\begin{bmatrix}0&0&0\\1&1&1\\1&0&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\1&1&0\\1&0&0\end{bmatrix},$$

相应的 $\hat{\sigma}(\bar{A})$分别为

$$\left\{\begin{bmatrix}1&1&1\\0&0&0\\0&1&1\end{bmatrix},\begin{bmatrix}1&1&1\\0&0&1\\0&1&0\end{bmatrix},\begin{bmatrix}1&1&0\\0&0&1\\0&1&1\end{bmatrix},\begin{bmatrix}1&0&1\\0&1&0\\0&1&1\end{bmatrix}\right\},$$

$$\left\{\begin{bmatrix}1&1&1\\0&0&1\\0&1&1\end{bmatrix}\right\}.$$

这时矩阵

$$\begin{array}{ccccc}
0\ 0\ 0\ 0 & 0\ 0\ 0\ 0 & 0\ 0\ 0\ 0 & 0\ 0\ 0\ 0 & 0\ 0\ 0\ 0\\
1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 & 1\ 1\ 0\ 0\\
1\ 0\ 0\ 0 & 1\ 0\ 0\ 0 & 1\ 0\ 0\ 0 & 1\ 0\ 0\ 0 & 1\ 0\ 0\ 0\\
1\ 1\ 1\ 1 & 1\ 1\ 1\ 1 & 1\ 1\ 0\ 1 & 1\ 0\ 1\ 1 & 1\ 1\ 1\ 1\\
0\ 0\ 0\ 1 & 0\ 0\ 1\ 1 & 0\ 0\ 1\ 1 & 0\ 1\ 0\ 1 & 0\ 0\ 1\ 1\\
0\ 1\ 1\ 1 & 0\ 1\ 0\ 1 & 0\ 1\ 1\ 1 & 0\ 1\ 1\ 1 & 0\ 1\ 1\ 1
\end{array}\qquad (5\text{-}3\text{-}16)$$

为 5 个(4, 1, 6)阶矩阵.

(4) 对 $\mathscr{F}_{4,1}(4,4)$作 A 矩阵为

$$\begin{bmatrix}0&0&0\\1&1&1\\1&0&0\\1&1&0\end{bmatrix},\quad\begin{bmatrix}0&0&0\\1&1&1\\0&0&1\\1&1&0\end{bmatrix},$$

相应的 $\tilde{\sigma}(\bar{A})$矩阵为

$$\left\{\begin{bmatrix}1&1&1\\0&0&0\\0&1&1\\0&0&1\end{bmatrix},\begin{bmatrix}1&0&1\\0&1&0\\0&1&1\\0&0&1\end{bmatrix}\right\},$$

$$\left\{\begin{bmatrix}1&1&1\\0&0&0\\1&1&0\\0&0&1\end{bmatrix},\begin{bmatrix}1&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix},\begin{bmatrix}1&1&1\\0&0&0\\0&1&0\\1&0&1\end{bmatrix},\begin{bmatrix}1&1&1\\0&0&0\\0&1&1\\1&0&0\end{bmatrix},\right.$$

$$\left.\begin{bmatrix}0&1&1\\1&0&0\\1&1&0\\0&0&1\end{bmatrix},\begin{bmatrix}0&1&1\\1&0&0\\0&1&0\end{bmatrix},\begin{bmatrix}1&0&1\\0&1&0\\1&1&0\\0&0&1\end{bmatrix},\begin{bmatrix}1&0&1\\0&1&0\\1&0&0\\0&1&1\end{bmatrix}\right\},$$

这时矩阵

$$
\begin{array}{cccccccccc}
0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0\\
1&1&1&0 & 1&1&1&0 & 1&1&1&0 & 1&1&1&0 & 1&1&1&0\\
1&0&0&0 & 1&0&0&0 & 0&0&1&0 & 0&0&1&0 & 0&0&1&0\\
1&1&0&0 & 1&1&0&0 & 1&1&0&0 & 1&1&0&0 & 1&1&0&0\\
1&1&1&1 & 1&0&1&1 & 1&1&1&1 & 1&1&1&1 & 1&1&1&1\\
0&0&0&1 & 0&1&0&1 & 0&0&0&1 & 1&0&0&1 & 0&0&0&1\\
0&1&1&1 & 0&1&1&1 & 1&1&0&1 & 0&1&0&1 & 0&1&0&1\\
0&0&1&1 & 0&0&1&1 & 0&0&1&1 & 0&0&1&1 & 1&0&1&1
\end{array}
$$

$$
\begin{array}{cccccccccc}
0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0 & 0&0&0&0\\
1&1&1&0 & 1&1&1&0 & 1&1&1&0 & 1&1&1&0 & 1&1&1&0\\
0&0&1&0 & 0&0&1&0 & 0&0&1&0 & 0&0&1&0 & 0&0&1&0\\
1&1&0&0 & 1&1&0&0 & 1&1&0&0 & 1&1&0&0 & 1&1&0&0\\
1&1&1&1 & 0&1&1&1 & 0&1&1&1 & 1&0&1&1 & 1&0&1&1\\
0&0&0&1 & 1&0&0&1 & 1&0&0&1 & 0&1&0&1 & 0&1&0&1\\
0&1&1&1 & 1&1&0&1 & 0&1&0&1 & 1&1&0&1 & 1&0&0&1\\
1&0&0&1 & 0&0&1&1 & 1&0&1&1 & 0&0&1&1 & 0&1&1&1
\end{array}
\tag{5-3-17}
$$

均为(4, 1, 8)阶矩阵.

(5) 对(5-3-13)～(5-3-14)的 29 个矩阵作

$$\beta_0 + \tau[D_a(C)]$$

运算,其中 $\beta_0 = 0, 1$; $a \subset \{1, \cdots, 4\}$, $\tau \in \mathrm{SYM}(4)$,则得到的全部(4, 1, r)阶矩阵, 相应的 $f(x^{(4)})$函数,即为全部 $\mathscr{F}_{4,1}$ 函数.

关于 $\mathscr{F}_{n,m}$ 函数的构造, 原则上仍可利用本节定理3 进行,但关于 m 阶反对偶矩阵的构造比 0 阶情形复杂得多. 例如对一阶反对偶的情形, 记 $A'[Q(a_j)]$ 为 $A[Q(a_j)]$ 划去第 j 列后的矩阵, 则 A, B 为一阶反对偶的充要条件为对任何 $j = 1, 2, \cdots, n$, $a_j \in F_2$,

$$A'[a(a_j)] \text{ 与 } B'[a(a_j)]$$

是反对偶的. 对此, 我们还没有找到一般性的判别与构造方法.

结　束　语

本书对非线性复杂度，M-序列的规范化构造，复合前馈序列的相关免疫性等一系列问题进行了探讨，相应的结果可供序列加密体制的构造与分析参考。有些问题如M-序列的直接构造问题，平均非线性复杂度估计的上、下界重合问题，(n, m)阶相关免疫函数在$m \geqslant 2$时的构造问题，复合序列的复杂性理论等问题，有待于进一步讨论解决，由于写作时间的仓促，错误与不足之处在所难免，希读者予以批评指正，笔者对此深为感谢。

参 考 文 献

[1] 万哲先，代数与编码，科学出版社，1979，第二版.

[2] 万哲先，代宗铎，刘木兰，冯绪宁，非线性移位寄存器，科学出版社，1978.

[3] 陶仁骥，关于 M-序列的补充，中国科学院数学研究所编码讨论班讲义，1975.

[4] 尹文霖，移位寄存器序列，四川人民出版社，1982.

[5] 高鸿勋，求全部 n 级 M-序列及其反馈函数的一个方法与证明，应用数学学报，2(1979)，316～324.

[6] 章照止，罗乔林，产生 M-序列的一个递推算法，系统科学与数学，7:4(1987)，335～343.

[7] 章照止，杨义先，关于周期为 2^n 的序列的复杂度分析，系统科学与数学，1990.

[8] C. 贝尔热著，李修睦译，图的理论及其应用，上海科学技术出版社，1963.

[9] 王梓坤，随机过程，科学出版社，1978.

[10] S. W. Golomb, Shift register sequences, Holden-Day Inc. San Francisco, 1967.

[11] A. H. Chan, R. A. Games and E. L. Key, On the complexities of Bruijn sequences, J. Combin. Theory, ser. A, 33(1982),233～246.

[11] R. A. 罗比著，朱甫臣等译，序列密码的设计与分析，1986.

[12] E. L Key, An analysais of the structure and complexity of nonlinear bemary sequence generatora, IEEE Trans Inform. Theory, Vol. IT-22, 6(1976), 732～736.

[13] P.Martin-Lof, The definition of random sequence, Jnform. and Control, 9(1966), 602～619.

[14] 丁石孙，线性移位寄存器序列，上海科学技术出版社，1982.

[15] 肖国镇，梁传甲，王育民，伪随机序列及其应用，国防工业出版社，1985.

[16] Alan. G. Konheim, Cryptography A primer, John Wily and Sons Inc., 1981.

[17] A.H. CHan, R.A. Games and E.L. Key, On the complexities of de Bruijn sequences, J. Combin.Theory.Ser.A, 33(1982), 233～246.

[18] T .Etzion and A.Lempel, On the distribution of de Brurjn sequen-

ces of given complexity, IEEE Trans.Inform. Theory, Vol. IT-30 4(1984), 611～614.

[19] 康庆德,GF(2)上M-序列构造方法,通信学报,4:4(1983),2～11.

[20] 熊荣华,M-序列反馈函数的构造方法,I,II,III,应用数学学报,9:2(1986),22～236;9:3(1986),339～351;11:3(1988),329～340.

[21] T.Siegenthaler, Cryptanalysists representation of nonlinearly filtered ML-sequences, Springer Lecture Notes, Eurocrypt, 1985.

[22] T.Siegenthaler, Correlation-Immunity of noniinearcombining function for cryptographic application, IEEET rans. Inform. Theory, Vol.IT-30, 5(1984),776～780.

[23] 沈世镒, 相关免疫函数判别与构造,通信学报,11:2(1990),68～72.

[24] Xiao Guochen, J.L.Massey, A spectral characterization of correlation-Immune combining function, IIEE Trans. Inform. Theory.

[25] 林须瑞,蔡长年,周期序列的复杂度分析,第三届全国密码会议.1988年, 西安.

[26] 林须瑞,序列密码及其复杂度分析,北京邮电学院,博士论文.

常用记号与术语

F_q：q 值的有限域。

a, b, c：F_q 中的元素。

$F_q^{(n)}$：F_q 域上的 n 维向量空间。

$a^{(n)} = (a_1, \cdots, a_n)$：$F_q^{(n)}$ 中的向量或 F_q 上的 n 维向量。

A, B, C：$F_q^{(n)}$ 中的子集或 F_q 上矩阵。

$\tilde{a} = (a_0, a_1, \cdots)$：$F_q$ 上的无穷序列。

$a(i, j) = (a_i, a_{i+1}, \cdots, a_j)$ $(i \leqslant j)$：$\tilde{a}$ 序列在区间 $[i, j]$ 上的向量段。

$N = \{1, 2, \cdots, n\}$：部分自然数集合。

$\alpha = \{i_1, i_2, \cdots, i_m\}$：$N$ 的子集，其中 $1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n$。

$\|A\|$：集合 A 的元素个数或矩阵 A 的行列式。

$\tilde{\alpha}_m$：全体 $\alpha \subset N, \|\alpha\| = m$ 的集合。

$a(\alpha) = (a_i, i \in \alpha) = (a_{i1}, \cdots, a_{im})$：$a^{(n)} = (a_1, a_2, \cdots, a_n)$ 在 α 上的部分向量。

$A \subset B$：A 集含于 B 集。

$a \in A$：元素 a 属于集合 A。

$A \cup B$，$A \cap B$，A/B，A^c：集合中的并，交，差，余运算。

$A + B$：A，B 互不相交时的并。

$A - B$：$B \subset A$ 时的差。

$A \otimes B$：A，B 的积。这时 $A \otimes B = \{(a, b): a \in A, b \in B\}$。

$\alpha^c = N - \alpha$：α 的余运算。

Φ：空集。

$F_q(\alpha)$：全体 $a(\alpha)$ 向量，为 $F_q^{(n)}$ 的部分向量空间。

$a + b$，$a \cdot b$（或 ab），$a - b$，a^b：F_q 域上的和，积，差，幂运算。

$\sum$，$\prod$：F_q 域上的连加，连乘运算或集合的连加，连乘运算。

$A \triangleq B$：B 为 A 的定义式。

$A \cong B$：A 与 B 近似相等。

$A \overset{*}{=} B$：在 B 式中的运算式为实数运算。

$a\oplus b$, $a\ominus b$, $a\odot b$, $a|b$: 实数中的的四则运算或集合运算。

$\sum^{*}$, $\prod^{*}$: 实数中的连加与连乘。

(由此可知,在实数中的运算有两种表示法,即如

$(a\oplus b)\odot c$ 一等价于$\overset{*}{=}(a+b)\cdot c$。

$$\sum_{i=1}^{n}{}^{*}a_i \text{ 等价于}\overset{*}{=}\sum_{i=1}^{n}a_i)$$

x, y: F_q 上取值的变元。

$x^{(n)}=(x,\cdots,x_n)$: F_q 上取值的 n 维多元向量(简称 n 元向量)。

$f(x)$: F_q 上的多项式函数。

$f(x_1,\cdots,x_n)$: F_q 上的 n 元非线性组合函数或布尔函数。

$\partial^{\circ}f(x)$, $\partial^{\circ}f(x^{(n)})$: $f(x)$ 与 $f(x^{(n)})$ 多项式的阶。

X, Y, Z: F_q 上取值的随机变量。

$X^{(n)}=(X_1,\cdots,X_n)$: n 维随机向量。

$\widetilde{X}=(X_0,X_1,\cdots)$: 随机序列。

$P_r\{X\in A\}$: X 属于 A 的概率。

$P_r\{X\in A/Y\in B\}$: 在 $Y\in B$ 的条件下, $X\in A$ 的概率。

$E[X]$: X 的数学期望(或均值)。

$D(X)$: 随机变量 X 的方差。

$g(X_1,\cdots,X_n)$: 随机变量 $X_1,\cdots,X_n$ 的函数。

$G=\{A,L\}$: 图,其中 A 为图中的全体顶点,L 为图中的全体弧。

s, t: 图中的点或状态。

S 或(s,t): G 图中的弧。

$G_n=\{A^{(n)},L^{(n)}\}$: de Bruijn-Good 有向图,其中$A^{(n)}=F_q^{(n)}$, $L^{(n)}=F_q^{(n+1)}$。

$G^{*}=\{A^{*},L^{*}\}$: G 图的倍图。

T_n: G_n 中的反树图。

T_{0n}: F_n 中的反干树图。

$\bar{a}$: F_2 域中 a 的补运算,即 $\bar{a}=1+a$。

$\bar{s}$: 状态 $s=(a_0,\cdots,a_{n-1})$ 的补运算,即 $\bar{s}=(\bar{a}_0,\bar{a},\cdots,\bar{a}_{n-1})$。

$\bar{A}$: 集合 A 的补运算,即

$$\bar{A}=\{\bar{s}=\bar{a}_0,\cdots,\bar{a}_{n-1}):\ s=(a_0,\cdots,a_{n-1})\in A\}。$$

s^{*}: 状态 $s=(a_0,a_1,\cdots,a_{n-1})$ 的共轭向量,即 $s^{*}=(\bar{a}_0,a_1,\cdots,a_{n-1})$

s'：状态 $s=(a_0, a_1, \cdots, a_{n-1})$的相伴向量，

即 $s'(a_0, a_1, \cdots, a_{n-2}, \bar{a}_{n-1})$。

$A=[a_{ij}]_{k\times n}$：$k\times n$ 阶矩阵。

E_n：$n\times n$ 阶么矩阵。

A^T：A 矩阵的转置。

ϕ_n：n维零向量 $\phi_n=(0, 0, \cdots, 0)$)。

I_n：n 维么元向量($I_n=(1, 1, \cdots, 1,)$)。

$e_i=(0, \cdots, 0, 1, 0, \cdots, 0)$：正交基向量。

$SYM(n)$：$N=\{1, 2, \cdots, n\}$ 上的置换群。

$\tau, \sigma\in SYM(n)$：N 上的置换运算。

$\tau(x_1, \cdots, x_n)=(x_{\tau(1)}, \cdots, x_{\tau(n)})$：$(x_1, \cdots, x_n)$向量的换位运算。

$C_L(a^{(p)})$，$C_L(\tilde{a})$：$a^{(p)}$，$\tilde{a}$ 的线性复杂度。

$C_N(a^{(p)}$，$C_N(\tilde{a})$：$a^{(p)}$，$\tilde{a}$ 的非线性复杂度。

$C_s(a^{(p)})$，$C_s(\tilde{a})$：$a^{(p)}$，$\tilde{a}$ 的非奇异复杂度。

$\langle l_p, f_p(x)\rangle$：$a^{(p)}$ 的线性移位寄存器综合解。

$\langle C_p, f_p(x^{(cp)})\rangle$：$a^{(p)}$ 的非线性移位器综合解。

q 值：F_q 中取值。

n级：线性，非线性移位寄存器的级数。

n元：多元多项式的变元数。

n阶：多项式的阶数，相关免疫函数的阶数。

$k\times n$阶：矩阵的阶数。

p 周期：序列的周期数。

(n, m)阶：n元，m阶相关免疫函数。